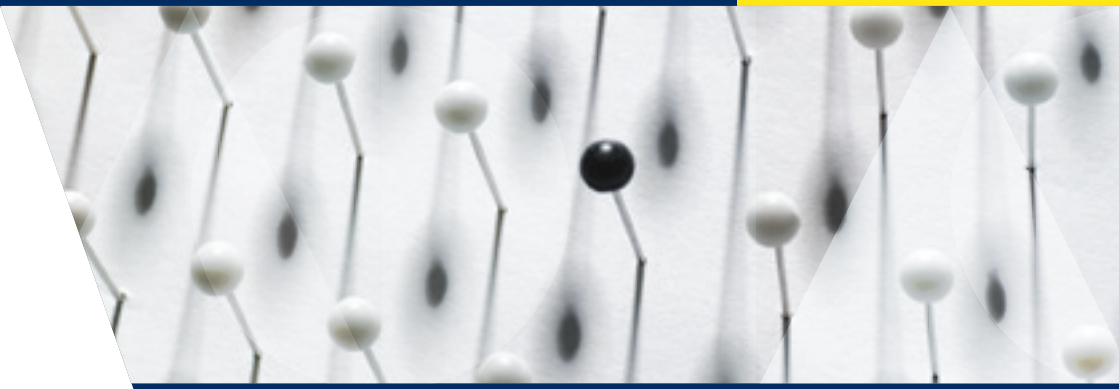
HANDBOOK



Handbook on European data protection law

2018 edition

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

The manuscript for this handbook was completed in April 2018.

Updates will become available in future on the FRA website at fra.europa.eu, the Council of Europe website at coe.int/dataprotection, on the European Court of Human Rights website under the Case Law menu at echr.coe.int, and on the European Data Protection Supervisor website at edps.europa.eu.

Photo credit (cover & inside): © iStockphoto

Luxembourg: Publications Office of the European Union, 2018

CoE:	ISBN 978-92-871-9849-5		
FRA – print:	ISBN 978-92-9491-903-8	doi:10.2811/58814	TK-05-17-225-EN-C
FRA – web:	ISBN 978-92-9491-901-4	doi:10.2811/343461	TK-05-17-225-EN-N

Printed by Imprimerie Centrale in Luxembourg

PRINTED ON PROCESS CHLORINE-FREE RECYCLED PAPER (PCF)

This handbook was drafted in English. The Council of Europe (CoE) and the European Court of Human Rights (ECtHR) take no responsibility for the quality of the translations into other languages. The views expressed in this handbook do not bind the CoE and the ECtHR. The handbook refers to a selection of commentaries and manuals. The CoE and ECtHR take no responsibility for their content, nor does their inclusion on this list amount to any form of endorsement of these publications. Further publications are listed on the internet pages of the ECtHR library at echr.coe.int.

The content of this handbook does not present an official position of the European Data Protection Supervisor (EDPS) and does not bind the EDPS in the exercise of his competences. The EDPS takes no responsibility for the quality of the translations into languages other than English.

Handbook on European data protection law

2018 edition

Foreword

Our societies are becoming ever more digitised. The pace of technological developments and how personal data are being processed affects each of us every day and in all sorts of ways in the light of these changes. Legal frameworks of the European Union (EU) and the Council of Europe that safeguard the protection of privacy and personal data have recently been reviewed.

Europe is at the forefront of data protection worldwide. The EU's data protection standards are based on Council of Europe Convention 108, EU instruments – including the General Data Protection Regulation and the Data Protection Directive for Police and Criminal Justice Authorities – as well as on the respective case law of the European Court of Human Rights and of the Court of Justice of the European Union.

The data protection reforms carried out by the EU and the Council of Europe are extensive and at times complex, with wide-ranging benefits and impact on individuals and businesses. This handbook aims to raise awareness and improve knowledge of data protection rules, especially among non-specialist legal practitioners who have to deal with data protection issues in their work.

The handbook has been prepared by the EU Agency for Fundamental Rights (FRA), with the Council of Europe (together with the Registry of the European Court of Human Rights) and the European Data Protection Supervisor. It updates a 2014 edition and is part of a series of legal handbooks co-produced by FRA and the Council of Europe.

We express our thanks to the data protection authorities of Belgium, Estonia, France, Georgia, Hungary, Ireland, Italy, Monaco, Switzerland and the United Kingdom for their helpful feedback on the draft version of the handbook. In addition, we express our appreciation to the European Commission's Data Protection Unit and its International Data Flows and Protection Unit. We thank the Court of Justice of the European Union for the documentary support provided during the preparatory works of this handbook.

Christos Giakoumopoulos	**Giovanni Buttarelli**	**Michael O'Flaherty**
Director General of Human Rights and Rule of Law Council of Europe	European Data Protection Supervisor	Director of the European Union Agency for Fundamental Rights

Contents

Abbreviations and acronyms

BCR	Binding corporate rule
CCTV	Closed circuit television
CETS	Council of Europe Treaty Series
Charter	Charter of Fundamental Rights of the European Union
CIS	Customs information system
CJEU	Court of Justice of the European Union (prior to December 2009, European Court of Justice, ECJ)
CoE	Council of Europe
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe). The amending Protocol (CETS No. 223) to Convention 108 was adopted by the Committee of Ministers of the Council of Europe on 18 May 2018 on the occasion of its 128th session held in Elsinore, Denmark. References to the 'Modernised Convention 108' refer to the Convention as amended by Protocol CETS No. 223.
CRM	Customer relations management
C-SIS	Central Schengen Information System
DPO	Data Protection Officer
DPA	Data Protection Authority
EAW	European Arrest Warrant
EDPB	European Data Protection Board
EC	European Community
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EFSA	European Food and Safety Authority
EFTA	European Free Trade Association
ENISA	European Network and Information Security Agency

ENU	Europol National Unit
EPPO	European Prosecutor's Office
ESMA	European Securities and Markets Authority
eTEN	Trans-European Telecommunication Networks
EU	European Union
EuroPriSe	European Privacy Seal
eu-LISA	EU Agency for Large-scale IT Systems
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
GPS	Global positioning system
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and communications technology
ISP	Internet service provider
JSB	Joint Supervisory Body
NGO	Non-governmental organisation
N-SIS	National Schengen Information System
OECD	Organisation for Economic Co-operation and Development
OJ	Official Journal
PIN	Personal identification number
PNR	Passenger name record
SCG	Supervision Coordination Group
SEPA	Single Euro Payments Area
SIS	Schengen Information System
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights
UN	United Nations
VIS	Visa Information System

How to use this handbook

This handbook outlines the legal standards relating to data protection set by the European Union (EU) and the Council of Europe (CoE). It is designed to assist practitioners not specialised in the field of data protection, including lawyers, judges and other legal practitioners, as well as individuals working for other bodies, such as non-governmental organisations (NGOs), who may be confronted with legal questions relating to data protection.

The handbook serves as a first point of reference on relevant EU law and the European Convention on Human Rights (ECHR), as well as the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and other CoE instruments.

Each chapter begins with a table that identifies the legal provisions relevant to the topics dealt with in the specific chapter. The tables cover both CoE and EU law, and include selected case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU). The relevant laws of the two different European orders, as they apply to the specific topics addressed, are then presented in sequence. This allows the reader to see where the two legal systems converge and where they differ. It should also help readers find the key information relating to their situation, especially if they are subject only to CoE law. In some chapters, where this helps the concise presentation of the content, the order of the topics in the tables may differ slightly from that within the chapter itself. The handbook also provides a brief overview of the United Nations framework.

Practitioners in non-EU states that are member states of the CoE and parties to the ECHR and Convention 108 can access the information relevant to their own country by going straight to the sections on the CoE. Practitioners in non-EU states must also bear in mind that, since the adoption of the EU General Data Protection Regulation, EU data protection rules apply to organisations and other entities that are not established in the EU, if they process personal data and offer goods and services to data subjects in the Union or monitor the behaviour of such data subjects.

Practitioners in EU Member States will need to consult both sections, as these states are bound by both legal orders. It should be noted that the reforms and modernisation of data protection rules in Europe, undertaken both in the framework of the Council of Europe (Modernised Convention 108 as amended by Protocol

CETS No. 223) and of the EU (adoption of the General Data Protection Regulation and of Directive 2016/680/EU), were carried out in parallel. Regulators in both legal systems have taken utmost care to ensure consistency and compatibility between the two legal frameworks. The reforms have thus brought greater harmonisation between CoE and EU data protection law. For individuals who need more information on a particular issue, a list of more specialised material can be found in the 'Further reading' section. For information regarding the provisions of Convention 108 and its additional Protocol of 2001, which continue to apply until the entry into force of the amending Protocol, readers should refer to the 2014 edition of the handbook.

CoE law is presented through short references to selected ECtHR cases. These have been chosen from the large number of ECtHR judgments and decisions that exist on data protection issues.

Relevant EU law comprises legislative measures that have been adopted, relevant provisions of the treaties and the Charter of Fundamental Rights of the European Union, as interpreted in the case law of the CJEU. In addition, the handbook presents opinions and guidelines adopted by the Article 29 Working Party, the advisory body tasked under the Data Protection Directive with providing expert advice to EU Member States, and that will be superseded by the European Data Protection Board (EDPB) from 25 May 2018 onwards. Opinions of the European Data Protection Supervisor also provide important insights into the interpretation of EU law and so are included in this handbook.

The cases described or cited in this handbook provide examples of an important body of both ECtHR and CJEU case law. The guidelines at the end of the handbook aim to assist readers in searching case law online. The CJEU case law presented relates to the former Data Protection Directive. However, the CJEU's interpretations remain applicable to the corresponding rights and obligations established by the General Data Protection Regulation.

In addition, practical illustrations with hypothetical scenarios are provided in textboxes with a blue background. These further illustrate the application of European data protection rules in practice, particularly where no specifically relevant ECtHR or CJEU case law exists. Other textboxes – with a grey background – provide examples taken from sources other than ECtHR and CJEU case law, such as legislation and opinions issued by the Article 29 Working Party.

The handbook begins with a brief description of the role of the two legal systems as established by the ECHR and EU law (Chapter 1). Chapters 2 to 10 cover the following issues:

- data protection terminology;
- key principles of European data protection law;
- rules of European data protection law;
- independent supervision;
- data subjects' rights and their enforcement;
- cross-border transfers and flows of personal data;
- data protection in the context of police and criminal justice;
- other European data protection rules in specific areas;
- modern challenges in personal data protection.

1

Context and background of European data protection law

EU	Issues covered	CoE
The right to data protection		
Treaty on the Functioning of the European Union, Article 16 Charter of Fundamental Rights of the European Union (the Charter), Article 8 (right to protection of personal data) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), OJ 1995 L 281 (in effect until May 2018) Council Framework Decision 2008/977/JHA on the protection of personal data processed in the context of police and judicial cooperation in criminal matters, OJ 2008 L 350 (in effect until May 2018) Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119 Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing		ECHR, Article 8 (right to respect for private and family life, home and correspondence) Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Modernised Convention 108)

EU	Issues covered	CoE
Council Framework Decision 2008/977/JHA (Data Protection for Police and Justice Authorities), OJ 2016 L 119 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L 201 Regulation (EC) No. 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (EU Institutions Data Protection Regulation), OJ 2001 L 8		
Limitations on the right to protection of personal data		
The Charter, Article 52 (1) General Data Protection Regulation, Article 23 CJEU, Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 2010		ECHR, Article 8 (2) Modernised Convention 108, Article 11 ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 2008
Balancing rights		
CJEU, Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 2010	In general	
CJEU, C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [GC], 2008 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014	Freedom of expression	ECtHR, *Axel Springer AG v. Germany* [GC], No. 39954/08, 2012 ECtHR, *Mosley v. the United Kingdom*, No. 48009/08, 2011 ECtHR, *Bohlen v. Germany*, No. 53495/09, 2015
CJEU, C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd* [GC], 2010 CJEU, C-615/13P, *ClientEarth, PAN Europe v. EFSA*, 2015	Access to documents	ECtHR, *Magyar Helsinki Bizottság v. Hungary* [GC], No. 18030/11, 2016
General Data Protection Regulation, Article 90	Professional secrecy	ECtHR, *Pruteanu v. Romania*, No. 30181/05, 2015
General Data Protection Regulation, Article 91	Freedom of religion or belief	

EU	Issues covered	CoE
	Freedom of arts and sciences	ECtHR, *Vereinigung bildender Künstler v. Austria*, No. 68345/01, 2007
CJEU, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [GC], 2008	Protection of property	
CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 2017	Economic rights	

1.1. The right to personal data protection

Key points

- Under Article 8 of the ECHR, a person's right to protection with respect to the processing of personal data forms part of the right to respect for private and family life, home and correspondence.
- CoE Convention 108 is the first and, to date, the only international legally binding instrument dealing with data protection. The Convention underwent a modernisation process, completed with the adoption of amending Protocol CETS No. 223.
- Under EU law, data protection has been acknowledged as a distinct fundamental right. It is affirmed in Article 16 of the Treaty of the Functioning of the EU, as well as in Article 8 of the EU Charter of Fundamental Rights.
- Under EU law, data protection was regulated for the first time by the Data Protection Directive in 1995.
- In view of rapid technological developments, the EU adopted new legislation in 2016 to adapt data protection rules to the digital age. The General Data Protection Regulation became applicable in May 2018, repealing the Data Protection Directive.
- Together with the General Data Protection Regulation, the EU adopted legislation on the processing of personal data by state authorities for law enforcement purposes. Directive (EU) 2017/680 establishes the data protection rules and principles that govern personal data processing for the purposes of preventing, investigating, detecting and prosecuting criminal offences or executing criminal penalties.

1.1.1. The right to respect for private life and the right to personal data protection: a brief introduction

The right to respect for private life and the right to personal data protection, although closely related, are distinct rights. The right to privacy – referred to in European law as the right to respect for private life – emerged in international human rights law in the Universal Declaration of Human Rights (UDHR), adopted in 1948, as one of the fundamental protected human rights. Soon after adoption of the UDHR, Europe too affirmed this right – in the European Convention on Human Rights (ECHR), a treaty that is legally binding on its Contracting Parties and that was drafted in 1950. The ECHR provides that everyone has the right to respect for his or her private and family life, home and correspondence. Interference with this right by a public authority is prohibited, except where the interference is in accordance with the law, pursues important and legitimate public interests and is necessary in a democratic society.

The UDHR and the ECHR were adopted well before the development of computers and the internet and the rise of the information society. These developments have brought considerable advantages to individuals and society, improving quality of life, efficiency and productivity. At the same time, they present new risks to the right to respect for private life. In response to the need for specific rules governing the collection and use of personal information, a new concept of privacy emerged, known in some jurisdictions as 'informational privacy' and in others as the 'right to informational self-determination'.[1] This concept led to the development of special legal regulations that provide personal data protection.

Data protection in Europe began in the 1970s, with the adoption of legislation – by some states – to control the processing of personal information by public authorities and large companies.[2] Data protection instruments were then established at

1 The German Federal Constitutional Court affirmed a right to informational self-determination in a 1983 judgment in *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1ff. The court considered informational self-determination to derive from the fundamental right to respect for personality, protected in the German Constitution. The ECtHR recognised in a 2017 judgment that Art. 8 of the ECHR "provides for the right to a form of informational self-determination". See ECtHR, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, No. 931/13, 27 June 2017, para. 137.

2 The German state of Hesse adopted the first law on data protection in 1970, which only applied in that state. In 1973, Sweden adopted the world's first national data protection law. By the end of the 1980s, several European states (France, Germany, the Netherlands and the United Kingdom) had also adopted legislation on data protection.

European level[3] and, over the years, data protection developed into a distinct value that is not subsumed by the right to respect for private life. In the EU legal order, data protection is recognised as a fundamental right, separate to the fundamental right to respect for private life. This separation raises the question of the relationship and differences between these two rights.

The right to respect for private life and the right to the protection of personal data are closely related. Both strive to protect similar values, i.e. the autonomy and human dignity of individuals, by granting them a personal sphere in which they can freely develop their personalities, think and shape their opinions. They are thus an essential prerequisite for the exercise of other fundamental freedoms, such as freedom of expression, freedom of peaceful assembly and association, and freedom of religion.

The two rights differ in their formulation and scope. The right to respect for private life consists of a general prohibition on interference, subject to some public interest criteria that can justify interference in certain cases. The protection of personal data is viewed as a modern and active right,[4] putting in place a system of checks and balances to protect individuals whenever their personal data are processed. The processing must comply with the essential components of personal data protection, namely independent supervision and the respect for the data subject's rights.[5]

Article 8 of the EU Charter of Fundamental Rights (the Charter) not only affirms the right to personal data protection, but also spells out the core values associated with this right. It provides that the processing of personal data must be fair, for specified purposes, and based on either the consent of the person concerned or a legitimate basis laid down by law. Individuals must have the right to access their personal data and to have it rectified, and compliance with this right must be subject to control by an independent authority.

---

3 The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was adopted in 1981. The EU adopted its first comprehensive data protection instrument in 1995: Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

4 Advocate General Sharpston described the case as involving two separate rights: the "classic" right to the protection of privacy and a more "modern" right, the right to data protection. See CJEU, Joined cases C-92/09 and C-93/02, *Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston*, 17 June 2010, para. 71.

5 Hustinx, P., EDPS Speeches & Articles, *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, July2013.

The right to personal data protection comes into play whenever personal data are processed; it is thus broader than the right to respect for private life. Any processing operation of personal data is subject to appropriate protection. Data protection concerns all kinds of personal data and data processing, irrespective of the relationship and impact on privacy. Processing of personal data may also infringe on the right to private life, as shown in the examples below. However, it is not necessary to demonstrate an infringement on private life for data protection rules to be triggered.

The right to privacy concerns situations where a private interest, or the "private life" of an individual, has been compromised. As demonstrated throughout this handbook, the concept of "private life" has been broadly interpreted in the case law, as covering intimate situations, sensitive or confidential information, information that could prejudice the perception of the public against an individual, and even aspects of one's professional life and public behaviour. However, the assessment of whether or not there is, or has been, an interference with "private life" depends on the context and facts of each case.

By contrast, any operation involving the processing of personal data could fall under the scope of data protection rules and trigger the right to personal data protection. For example, where an employer records information relating to the names of and remuneration paid to employees, the mere recording of this information cannot be regarded as an interference with private life. Such an interference could, however, be argued if, for instance, the employer transferred the employees' personal information to third parties. Employers must in any case comply with data protection rules because recording employees' information constitutes data processing.

Example: In *Digital Rights Ireland,*[6] the CJEU was called upon to decide on the validity of Directive 2006/24/EC in light of the fundamental rights to personal data protection and respect for private life, affirmed in the EU Charter of Fundamental Rights. The directive required providers of publicly available electronic communication services or public communication networks to retain citizens' telecommunication data for up to two years, to ensure that the data were available for the purposes of preventing, investigating and prosecuting serious crime. The measure only concerned metadata, location data and data necessary to identify the subscriber or user. It did not apply to the content of electronic communications.

6 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [GC], 8 April 2014.

The CJEU deemed the directive an interference with the fundamental right to personal data protection "because it provides for the processing of personal data".[7] In addition, it found that the directive interfered with the right to respect of private life.[8] When taken as a whole, the personal data retained pursuant to the directive, which could be accessed by competent authorities, could allow "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them".[9] The interference with the two rights was wide-ranging and particularly serious.

The CJEU declared Directive 2006/24/EC invalid, finding that even though it pursued a legitimate aim, the interference with the rights to personal data protection and private life was serious and not limited to what was strictly necessary.

1.1.2. International legal framework: United Nations

The United Nations framework does not recognise personal data protection as a fundamental right, although the right to privacy is a long-established fundamental right in the international legal order. Article 12 of the UDHR on respect for private and family life[10] marked the first time an international instrument laid down an individual's right to protection of their private sphere against intrusion from others, especially from the state. Though a non-binding declaration, the UDHR has considerable status as the foundational instrument of international human rights law, and has influenced the development of other human rights instruments in Europe. The International Covenant on Civil and Political Rights (ICCPR) entered into force in 1976. It proclaims that no one may be subjected to arbitrary or unlawful interference with their privacy, home or correspondence, nor to unlawful attacks on their honour and reputation. The ICCPR is an international treaty that commits its 169 parties to respecting and ensuring the exercise of individuals' civil rights, including privacy.

7 *Ibid.*, para. 36.

8 *Ibid.*, paras. 32-35.

9 *Ibid.*, para. 27.

10 United Nations (UN), Universal Declaration of Human Rights (UDHR), 10 December 1948.

Since 2013, the United Nations has adopted two resolutions on privacy issues entitled "the right to privacy in the digital age"[11] in response to the development of new technologies and to revelations on mass surveillance undertaken in some states (the Snowden revelations). They strongly condemn mass surveillance and highlight the impact such surveillance can have on the fundamental rights to privacy and freedom of expression, and on the functioning of a vibrant and democratic society. Though not legally binding, they sparked an important international, high-level political debate about privacy, new technologies and surveillance. They also led to the establishment of a Special Rapporteur on the right to privacy, with a mandate to promote and protect this right. The rapporteur's specific tasks include gathering information on national practices and experiences in relation to privacy and the challenges arising from new technologies, the exchange and promotion of best practice, and identifying potential obstacles.

While earlier resolutions focused on the negative effects of mass surveillance and the responsibility of states to constrain the powers of intelligence authorities, more recent resolutions reflect a key development in the debate on privacy in the United Nations.[12] The resolutions adopted in 2016 and 2017 reaffirm the need to limit the powers of intelligence agencies and condemn mass surveillance. However, they also explicitly state that "the increasing capabilities of business enterprises to collect, process and use personal data can pose a risk to the enjoyment of the right to privacy in the digital age". Thus, in addition to the responsibility of state authorities, the resolutions point to the private sector's responsibility to respect human rights, and call for companies to inform users about the collection, use, sharing and retention of personal data and to establish transparent processing policies.

1.1.3. The European Convention on Human Rights

The Council of Europe was formed in the aftermath of the Second World War to bring together the states of Europe to promote the rule of law, democracy, human rights and social development. For this purpose, it adopted the ECHR in 1950, which entered into force in 1953.

11 See UN, General Assembly, Resolution on the right to privacy in the digital age, A/RES/68/167, New York, 18 December 2013; and UN, General Assembly, Revised draft resolution on the right to privacy in the digital age, A/C.3/69/L.26/Rev.1, New York, 19 November 2014.

12 UN, General Assembly, Revised draft resolution on the right to privacy in the digital age, A/C.3/71/L.39/Rev.1, New York, 16 November 2016; UN, Human Rights Council, The right to privacy in the digital age, A/HRC/34/L.7/Rev.1, 22 March 2017.

Contracting Parties have an international obligation to comply with the ECHR. All CoE member states have now incorporated or given effect to the ECHR in their national law, which requires them to act in accordance with the convention's provisions. Contracting Parties must respect the rights stipulated in the convention when exercising any activity or power. This includes activities undertaken for national security. Landmark judgments of the European Court of Human Rights (ECtHR) have involved state activities in the sensitive areas of national security law and practice.[13] The Court has not hesitated to affirm that surveillance activities constitute an interference with the respect for private life.[14]

To ensure that the Contracting Parties observe their obligations under the ECHR, the ECtHR was set up in Strasbourg, France in 1959. The ECtHR ensures that states observe their obligations under the Convention by considering complaints from individuals, groups of individuals, NGOs or legal persons alleging violations of the convention. The ECtHR can also examine inter-state cases brought by one or more CoE member states against another member state.

As of 2018, the Council of Europe comprises 47 Contracting Parties, 28 of which are also EU Member States. An applicant before the ECtHR does not need to be a national of one of the Contracting Parties, although alleged violations must take place within the jurisdiction of one of the Contracting Parties.

The right to personal data protection forms part of the rights protected under Article 8 of the ECHR, which guarantees the right to respect for private and family life, home and correspondence, and lays down the conditions under which restrictions of this right are permitted.[15]

The ECtHR has examined many situations involving data protection issues. These include interception of communications,[16] various forms of surveillance by both the private and public sectors,[17] and protection against storage of personal data

13 See, for example: ECtHR, *Klass and Others v. Germany*, No. 5029/71, 6 September 1978; ECtHR, *Rotaru v. Romania* [GC], No. 28341/95, 4 May 2000 and ECtHR, *Szabó and Vissy v. Hungary*, No. 37138/14, 12 January 2016.

14 *Ibid*.

15 Council of Europe, European Convention on Human Rights, CETS No. 005, 1950.

16 See, for example: ECtHR, *Malone v. the United Kingdom*, No. 8691/79, 2 August 1984; ECtHR, *Copland v. the United Kingdom*, No. 62617/00, 3 April 2007, or ECtHR, *Mustafa Sezgin Tanrıkulu v. Turkey*, No. 27473/06, 18 July 2017.

17 See, for example: ECtHR, *Klass and Others v. Germany*, No. 5029/71, 6 September 1978; ECtHR, *Uzun v. Germany*, No. 35623/05, 2 September 2010.

by public authorities.[18] The respect for private life is not an absolute right, as the exercise of the right to privacy could compromise other rights, such as freedom of expression and access to information and vice versa. Hence, the Court strives to find a balance between the different rights at stake. It has clarified that Article 8 of the ECHR not only obliges states to refrain from any actions that might violate this convention right, but that they are in certain circumstances also under positive obligations to actively secure effective respect for private and family life.[19] The appropriate chapters describe many of these cases in detail.

1.1.4. Council of Europe Convention 108

With the emergence of information technology in the 1960s, there was a growing need for more detailed rules to safeguard individuals by protecting their personal data. By the mid-1970s, the Committee of Ministers of the Council of Europe adopted various resolutions on personal data protection, referring to Article 8 of the ECHR.[20] In 1981, a Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108)[21] was opened for signature. Convention 108 was, and still remains, the only legally binding international instrument in the data protection field.

Convention 108 applies to all data processing carried out by both the private and public sectors, including data processing by the judiciary and law enforcement authorities. It protects individuals against abuses that may accompany the processing of personal data, and seeks, at the same time, to regulate the transborder flows of personal data. As regards the processing of personal data, the principles laid down in the convention concern, in particular, fair and lawful collection and automatic processing of data, for specified legitimate purposes. This means that the data should not be used for ends incompatible with these purposes and should be kept for no longer than is necessary. They also concern the quality of the data, in

18 See, for example: ECtHR, *Roman Zakharov v. Russia*, No. 47143/06, 4 December 2015; ECtHR, *Szabó and Vissy v. Hungary*, No. 37138/14, 12 January 2016.

19 See for example: ECtHR, *I v. Finland*, No. 20511/03, 17 July 2008; ECtHR, *K.U. v. Finland*, No. 2872/02, 2 December 2008.

20 Council of Europe, Committee of Ministers (1973), Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, 26 September 1973; Council of Europe, Committee of Ministers (1974), Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, 20 September 1974.

21 Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 1981.

particular that they must be adequate, relevant and not excessive (proportionality), as well as accurate.

In addition to providing guarantees on the processing of personal data and data security obligations, it outlaws, in the absence of proper legal safeguards, the processing of 'sensitive' data – such as on a person's race, politics, health, religion, sexual life or criminal record.

The convention also enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected. Restrictions on the rights laid down in the convention are possible only when overriding interests, such as state security or defence, are at stake. In addition, the convention provides for the free flow of personal data between its Contracting Parties and imposes some restrictions on flows to states where legal regulation does not provide equivalent protection.

It should be noted that Convention 108 is binding for states that have ratified it. It is not subject to the judicial supervision of the ECtHR, but has been taken into consideration in the case law of the ECtHR within the context of Article 8 of the ECHR. Over the years, the Court has ruled that personal data protection is an important part of the right to respect for private life (Article 8), and has been guided by the principles of Convention 108 in determining whether or not there has been an interference with this fundamental right.[22]

To further develop the general principles and rules laid down in Convention 108, the CoE's Committee of Ministers adopted several non-legally binding recommendations. These recommendations have influenced the development of data protection law in Europe. For example, for years, the only instrument in Europe providing guidance on the use of personal data in the police sector was the Police Recommendation.[23] The principles contained in the recommendation, such as the means of retaining data files and the need to implement clear rules on the persons allowed access to those files, were further developed and are reflected in the subsequent EU legislation.[24] More recent recommendations seek to address the challenges of the

22 See, for example: ECtHR, *Z v. Finland*, No. 22009/93, 25 February 1997.

23 Council of Europe, Committee of Ministers (1987), Recommendation Rec(87)15 to member states regulating the use of personal data in the police sector, Strasbourg, 17 September 1987.

24 Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23 November 1995.

digital age – for instance, in relation to data processing in the context of employment (see Chapter 9).

All EU Member States have ratified Convention 108. In 1999, amendments to Convention 108 were proposed to enable the EU to become a party but never entered into force.[25] In 2001, an Additional Protocol to Convention 108 was adopted. It introduced provisions on transborder data flows to non-parties, so-called third countries, and on the mandatory establishment of national data protection supervisory authorities.[26]

Convention 108 is open for accession by non-Contracting Parties of the CoE. The Convention's potential as a universal standard, together with its open character, serve as a basis for promoting data protection at global level. To date, 51 countries are parties to Convention 108. They include all member states of the Council of Europe (47 countries); Uruguay, the first non-European country to accede in August 2013; and Mauritius, Senegal and Tunisia, which acceded in 2016 and 2017.

The convention recently underwent a process of modernisation. A public consultation carried out in 2011 confirmed the two main objectives of that work: reinforcing the protection of privacy in the digital arena and strengthening the convention's follow-up mechanism. The modernisation process focused on these objectives and was completed with the adoption of a protocol amending Convention 108 (Protocol CETS No. 223). The work was carried out in parallel with other reforms to international data protection instruments, and alongside the reform of EU data protection rules, launched in 2012. Regulators at the Council of Europe and EU level have taken the utmost care to ensure consistency and compatibility between the two legal frameworks. The modernisation preserves the convention's general and flexible character and reinforces its potential as a universal instrument on data protection law. It reaffirms and stabilises important principles and provides new rights to individuals, while simultaneously increasing the responsibilities of entities that process personal data and ensuring greater accountability. For example, individuals whose personal data are being processed have the right to obtain knowledge of the reasoning of such data processing and the right to object to that processing. To counter

25 Council of Europe, Amendments to the Convention for the protection of individuals with regard to automatic processing of Personal Data (ETS No. 108) adopted by the Committee of Ministers, in Strasbourg, on 15 June 1999.

26 Council of Europe, Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows, CETS No. 181, 2001. With the modernisation of Convention 108, this Protocol is no longer applied as its provisions have been updated and integrated into the Modernised Convention 108.

the increased use of profiling in the online world, the convention also establishes the right of the individual not to be subject to decisions solely based on automated processing without having their own views taken into consideration. Effective enforcement of data protection rules by independent supervisory authorities in the Contracting Parties is considered central to the convention's practical implementation. To this end, the modernised convention underlines the need for supervisory authorities to be vested with effective powers and functions and to enjoy genuine independence when fulfilling their mission.

1.1.5. European Union data protection law

EU law is composed of primary and secondary EU law. The treaties, namely the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU), have been ratified by all EU Member States; they form 'primary EU law'. The regulations, directives and decisions of the EU have been adopted by the EU institutions that have been given such authority under the treaties; they constitute 'secondary EU law'.

Data protection in primary EU law

The original treaties of the European Communities did not contain any reference to human rights or their protection, given that the European Economic Community was initially envisaged as a regional organisation focused on economic integration and the establishment of a common market. A fundamental principle underpinning the creation and development of the European Communities – and one which is equally valid today – is the principle of conferral. According to this principle, the EU acts only within the limits of the competences conferred upon it by the Member States, as reflected in the EU treaties. In contrast to the Council of Europe, the EU treaties include no explicit competence on fundamental rights matters.

As cases came before the CJEU alleging human rights violations in areas within the scope of EU law, however, the CJEU provided an important interpretation of the treaties. To grant protection to individuals, it brought fundamental rights into the so-called general principles of European law. According to the CJEU, these general principles reflect the content of human rights protection found in national constitutions and human rights treaties, in particular the ECHR. The CJEU stated that it would ensure compliance of EU law with these principles.

In recognising that its policies could have an impact on human rights and in an effort to make citizens feel 'closer' to the EU, the EU in 2000 proclaimed the Charter of

Fundamental Rights of the European Union (Charter). It incorporates the whole range of civil, political, economic and social rights of European citizens, by synthesising the constitutional traditions and international obligations common to the Member States. The rights described in the Charter are divided into six sections: dignity, freedoms, equality, solidarity, citizens' rights and justice.

Originally only a political document, the Charter became legally binding[27] as EU primary law (see Article 6 (1) of the TEU) when the Lisbon Treaty came into force on 1 December 2009.[28] The provisions of the Charter are addressed to EU institutions and bodies, obliging them to respect the rights listed therein while fulfilling their duties. The Charter's provisions also bind Member States when they implement EU law.

The Charter not only guarantees the respect for private and family life (Article 7), but also establishes the right to the protection of personal data (Article 8). The Charter explicitly raises the level of this protection to that of a fundamental right in EU law. EU institutions and bodies must guarantee and respect this right, as do Member States when implementing Union law (Article 51 of the Charter). Formulated several years after the Data Protection Directive, Article 8 of the Charter must be understood as embodying pre-existing EU data protection law. The Charter, therefore, not only explicitly mentions a right to data protection in Article 8 (1), but also refers to key data protection principles in Article 8 (2). Finally, Article 8 (3) of the Charter requires an independent authority to control the implementation of these principles.

The adoption of the Lisbon Treaty is a landmark in the development of data protection law, not only for elevating the Charter to the status of a binding legal document at the level of primary law, but also for providing for the right to personal data protection. This right is specifically provided for in Article 16 of the TFEU, under the part of the treaty dedicated to the general principles of the EU. Article 16 also creates a new legal basis, granting the EU the competence to legislate on data protection matters. This is an important development because EU data protection rules – notably the Data Protection Directive – were initially based on the internal market legal basis, and on the need to approximate national laws so that the free movement of data within the EU was not inhibited. Article 16 of the TFEU now provides an independent legal basis for a modern, comprehensive approach to data protection, which covers all matters

27 EU (2012), Charter of Fundamental Rights of the European Union, OJ 2012 C 326.

28 See consolidated versions of European Communities (2012), Treaty on European Union, OJ 2012 C 326; and of European Communities (2012), TFEU, OJ 2012 C 326.

of EU competence, including police and judicial cooperation in criminal matters. Article 16 of the TFEU also affirms that compliance with data protection rules adopted pursuant to it must be subject to the control of independent supervisory authorities. Article 16 served as a legal basis for the adoption of the comprehensive reform of data protection rules in 2016, i.e. the General Data Protection Regulation and the Data Protection Directive for Police and Criminal Justice Authorities (see below).

The General Data Protection Regulation

From 1995 until May 2018, the principal EU legal instrument on data protection was Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive).[29] It was adopted in 1995, at a time when several Member States had already adopted national data protection laws,[30] and emerged from the need to harmonise these laws to ensure a high level of protection and the free flow of personal data among the different Member States. Free movement of goods, capital, services and people within the internal market required the free flow of data, which could not be realised unless the Member States could rely on a uniform high level of data protection.

The Data Protection Directive reflected the data protection principles already contained in national laws and in Convention 108, while often expanding them. It drew on the possibility, provided for in Article 11 of Convention 108, of adding on instruments of protection. In particular, the introduction in the directive of independent supervision as an instrument for improving compliance with data protection rules proved to be an important contribution to the effective functioning of European data protection law. Consequently, this feature was incorporated into CoE law in 2001 by the Additional Protocol to Convention 108. This illustrates the close interaction and positive influence of the two instruments upon one another over the years.

The Data Protection Directive established a detailed and comprehensive data protection system in the EU. However, in accordance with the EU legal system,

29 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281.

30 The German state of Hesse adopted the world's first data protection law in 1970, which only applied to that state. Sweden adopted the *Datalagen* in 1973; Germany adopted the *Bundesdatenschutzgestez* in 1976; and France adopted the *Loi relatif à l'informatique, aux fichiers et aux libertés* in 1977. In the United Kingdom, the Data Protection Act was adopted in 1984. Finally, the Netherlands adopted the *Wet Persoonregistraties* in 1989.

directives do not apply directly and must be transposed into the national laws of the Member States. Inevitably, Member States have a margin of discretion in transposing the directive's provisions. Even though the directive was meant to provide complete harmonisation[31] (and a full level of protection), in practice it was transposed differently in the Member States. This resulted in the establishment of diverse data protection rules across the EU, with definitions and rules interpreted differently in national laws. The levels of enforcement and the severity of sanctions also varied across the Member States. Finally, there were significant changes in information technology since the drafting of the directive in the mid-1990s. Taken together, these reasons prompted the reform of EU data protection legislation.

The reform led to the adoption of the General Data Protection Regulation in April 2016, after years of intense discussion. The debates on the need to modernise EU data protection rules began in 2009, when the Commission launched a public consultation about the future legal framework for the fundamental right to personal data protection. The proposal for the regulation was published by the Commission in January 2012, starting a long legislative process of negotiations between the European Parliament and the Council of the EU. After adoption, the General Data Protection Regulation provided for a two year-transitional period. It became fully applicable on 25 May 2018, when the Data Protection Directive was repealed.

The adoption of the General Data Protection Regulation in 2016 modernised EU data protection legislation, making it fit for protecting fundamental rights in the context of the digital age's economic and social challenges. The GDPR preserves and develops the core principles and rights of the data subject provided for in the Data Protection Directive. In addition, it introduced new obligations requiring organisations to implement data protection by design and by default; to appoint a Data Protection Officer in certain circumstances; to comply with a new right to data portability; and to comply with the principle of accountability. Under EU law, regulations are directly applicable; there is no need for national implementation. The General Data Protection Regulation thus provides for a single set of data protection rules across the EU. This creates consistent data protection rules throughout the EU, establishing an environment of legal certainty from which economic operators and individuals as "data subjects" may benefit.

However, even though the General Data Protection Regulation is directly applicable, Member States are expected to update their existing national data protection laws

31 CJEU, Joined cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 November 2011, para. 29.

to fully align with the regulation, while also reflecting a margin of discretion for specific provisions in recital 10. The main rules and principles established in the regulation, and the strong rights it affords to individuals, form a large part of the handbook and are presented in the following chapters. The regulation has comprehensive rules on territorial scope. It applies to businesses established in the EU, and also applies to controllers and processors not established in the EU that offer goods or services to data subjects in the EU or monitor their behaviour. As several overseas technology businesses have a key share in the European market and millions of EU customers, subjecting these organisations to EU data protection rules is important to ensure the protection of individuals, as well as to ensure a level playing field.

Data protection in law enforcement – Directive 2016/680

The repealed Data Protection Directive provided a comprehensive data protection regime. This regime has now been further enhanced with the adoption of the General Data Protection Regulation. Though comprehensive, the repealed Data Protection Directive's scope of application was limited to activities that fall under the internal market, and to activities of public authorities other than law enforcement. Adoption of special instruments was thus required to achieve the necessary clarity and balance between data protection and other legitimate interests and to meet challenges that are particularly pertinent in specific sectors. This is the case for rules governing the processing of personal data by law enforcement authorities.

The first EU legal instrument to regulate this matter was Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. Its rules applied only to police and judicial data when exchanged between Member States. Domestic processing of personal data by law enforcement was excluded from its scope of application.

Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data,[32] referred to as the Data Protection Directive for Police and Criminal Justice Authorities, remedied this situation. Adopted in parallel with the General Data Protection Regulation, the

32 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, OJ L 119, 4 May 2016.

directive repealed Framework Decision 2008/977/JHA and established a comprehensive system of personal data protection in the context of law enforcement, while also acknowledging the particularities of public security-related data processing. While the General Data Protection Regulation lays down general rules to protect individuals in relation to the processing of their personal data, and to ensure the free movement of such data within the EU, the directive lays down specific rules for data protection in the fields of judicial cooperation in criminal matters and police cooperation. Where a competent authority processes personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences, Directive 2016/680 will apply. Where competent authorities process personal data for purposes other than the abovementioned ones, the general regime under the General Data Protection Regulation will apply. Unlike its predecessor (Council Framework Decision 2008/977/JHA), the scope of application of Directive 2016/680 extends to domestic processing of personal data by law enforcement authorities and is not limited to the exchanges of such data between Member States. In addition, the directive seeks to achieve a balance between the rights of individuals and the legitimate objectives of security-related processing.

To this end, the directive affirms the right to personal data protection and the core principles that should cover data processing, closely following the rules and principles enshrined in the General Data Protection Regulation. The rights of individuals and the obligations imposed on controllers – for example, in relation to data security, data protection by design and by default, and data breach notifications – resemble the rights and obligations in the General Data Protection Regulation. The directive also takes into consideration, and tries to address, serious emerging technological challenges that can have a particularly onerous impact on individuals, such as the use of profiling techniques by law enforcement authorities. In principle, decisions based solely on automated processing, including profiling, must be prohibited.[33] In addition, they must not be based on sensitive data. Such principles are subject to certain exceptions provided in the directive. Additionally, such processing must not result in discrimination against any person.[34]

The directive also contains rules to ensure the accountability of controllers. They must designate a data protection officer to monitor compliance with the data protection rules, to inform and advise the entity and employees carrying out the processing of their obligations, and to cooperate with the supervisory authority.

33 Data Protection Directive for Police and Criminal Justice Authorities, Art. 11 (1).

34 *Ibid.*, Art. 11 (2) and (3).

Processing of personal data in the police and criminal justice sector is now subject to the supervision of independent supervisory authorities. Both the general data protection legal regime and the special data protection regime for law enforcement and criminal matters must equally comply with the requirements of the EU Charter of Fundamental Rights.

The special regime for data processing in the context of police and judicial cooperation established by the Data Protection Directive for Police and Criminal Justice Authorities is described in detail in Chapter 8.

Directive on privacy and electronic communications

The establishment of special data protection rules was also deemed necessary in the sector of electronic communications. With the development of the internet, landline and mobile telephony, it was important to ensure that users' rights to privacy and confidentiality would be respected. Directive 2002/58/EC[35] concerning the processing of personal data and the protection of privacy in electronic communications (Directive on privacy and electronic communications or e-Privacy Directive) sets out rules on the security of personal data in these networks, the notification of personal data breaches, and the confidentiality of communications.

In respect of security, electronic communication services operators must, among other things, ensure that access to personal data is limited solely to authorised persons and take measures to prevent personal data from being destroyed, lost or accidentally damaged.[36] Where there is a particular risk of breach of the security of the public communications network, operators must inform the subscribers about the risk.[37] If, despite the security measures implemented, a breach of security occurs, operators must notify the competent national authority entrusted with implementation and enforcement of the directive of the personal data breach. Operators are sometimes required to also notify personal data breaches to individuals, namely where the breach is likely to negatively affect their personal data or privacy.[38] The confidentiality of communications requires that the listening, tapping, storage or any type of surveillance or interception of communications and metadata is, in principle,

35 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications, OJ L 201 (Directive on privacy and electronic communications or e-Privacy Directive).

36 Directive on privacy and electronic communications, Art. 4 (1).

37 *Ibid*., Art. 4 (2).

38 *Ibid*., Art. 4 (3).

prohibited. The directive also bans unsolicited communications (often referred to as "spam"), unless the users have given their consent, and contains rules on the storage of "cookies" on computers and devices. These core negative obligations clearly indicate that confidentiality of communications is significantly linked to the protection of the right to respect for private life enshrined in Article 7 of the Charter and the right to personal data protection enshrined in Article 8 of the Charter.

In January 2017, the Commission published a proposal for a regulation concerning the respect for private life and the protection of personal data in electronic communications, meant to replace the e-Privacy Directive. The reform aims to align the rules governing electronic communications with the new data protection regime established under the General Data Protection Regulation. The new regulation will be directly applicable throughout the EU; all individuals will enjoy the same level of protection of their electronic communications, while telecommunication operators and businesses will benefit from clarity, legal certainty and the existence of a single set of rules across the EU. The proposed rules on confidentiality of electronic communications will also apply to new players providing electronic communication services which are not covered by the e-Privacy Directive. The latter only covered traditional telecommunication services providers. With a massive uptake in the use of services such as Skype, WhatsApp, Facebook Messenger and Viber to send messages or call, these over-the-top (OTT services) will now fall within the scope of the regulation and will have to comply with its requirements on data protection, privacy and security. At the time of publication of this handbook, a legislative process on the e-Privacy rules was still ongoing.

Regulation No. 45/2001

As the Data Protection Directive could apply only to EU Member States, an additional legal instrument was needed to establish data protection for the processing of personal data by EU institutions and bodies. Regulation (EC) No. 45/2001 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data (EU Institutions Data Protection Regulation) fulfils this task.[39]

Regulation No. 45/2001 closely follows the principles of the general EU data protection regime, and applies those principles to data processing carried out by EU

39 Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, OJ 2001 L 8.

institutions and bodies in the exercise of their functions. In addition, it establishes an independent supervisory authority to monitor the application of its provisions, the European Data Protection Supervisor (EDPS). The EDPS is vested with supervisory powers and the duty to monitor the processing of personal data in the EU institutions and bodies, and to hear and investigate complaints for alleged breaches of the data protection rules. It also provides advice to EU institutions and bodies on all matters concerning personal data protection, ranging from proposals for new legislation to the drawing up of internal rules relating to data-processing.

In January 2017, the European Commission presented a proposal for a new regulation on data processing by EU institutions, which will repeal the current regulation. As with the reform of the e-Privacy Directive, the reform of Regulation No. 45/2001 will modernise and align its rules with the new data protection regime established under the General Data Protection Regulation.

The role of the CJEU

The CJEU has jurisdiction in determining whether or not a Member State has fulfilled its obligations under EU data protection law, and in interpreting EU legislation to ensure its effective and uniform application throughout the Member States. Since adoption of the Data Protection Directive in 1995, a considerable body of case law has accumulated, clarifying the scope and meaning of the data protection principles and the fundamental right to personal data protection as enshrined in Article 8 of the Charter. Even though the directive has been repealed and a new legal instrument – the General Data Protection Regulation – is now in force, that pre-existing case law remains relevant and valid for the interpretation and application of EU data protection principles, to the extent that the core principles and concepts of the Data Protection Directive were kept in the GDPR.

1.2. Limitations on the right to personal data protection

Key points

- The right to personal data protection is not an absolute right; it may be limited if necessary for an objective of general interest or to protect the rights and freedoms of others.

- The conditions for limiting the rights to respect for private life and to personal data protection are listed in Article 8 of the ECHR and Article 52 (1) of the Charter. They have been developed and interpreted through the case law of the ECtHR and the CJEU.
- Under CoE data protection law, processing personal data constitutes lawful interference with the right to respect for private life and can only be carried out if it:
  - is in accordance with the law;
  - pursues a legitimate aim;
  - respects the essence of the fundamental rights and freedoms;
  - is necessary and proportionate in a democratic society to achieve a legitimate purpose.
- The EU legal order places similar conditions on limitations on the exercise of the fundamental rights protected by the Charter. Any limitation to any fundamental right, including to personal data protection, can be lawful only if it:
  - is in accordance with the law;
  - respects the essence of the right;
  - subject to the principle of proportionality, is necessary; and
  - pursues an objective of general interest recognised by the EU, or the need to protect the rights of others.

The fundamental right to personal data protection under Article 8 of the Charter is not an absolute right, "but must be considered in relation to its function in society".[40] Article 52 (1) of the Charter thus recognises that limitations may be imposed on the exercise of rights such as those set forth in Articles 7 and 8 of the Charter, as long as those limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.[41] Similarly, in the ECHR system, data protection is guaranteed by Article 8, and the exercise of that right may be limited where necessary to pursue a legitimate purpose. This section refers to the conditions for interference under the ECHR, as interpreted by the case law of the ECtHR, as well as the conditions for lawful limitations under Article 52 of the Charter.

40 See, for example, CJEU, Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 9 November 2010, para. 48.

41 *Ibid.*, para. 50.

1.2.1. Requirements for justified interference under the ECHR

Processing personal data may constitute an interference with the data subject's right to respect for private life, protected by Article 8 of the ECHR.[42] As explained above (see Section 1.1.1 and Section 1.1.4.), contrary to the EU legal order, the ECHR does not affirm personal data protection as a distinct fundamental right. Rather, personal data protection forms part of the rights protected under the right to respect for private life. Thus, not any operation involving the processing of personal data could fall under the scope of Article 8 of the ECHR. For Article 8 to be triggered, it first has to be determined whether a private interest, or a person's private life, have been compromised. Through its case law, the ECtHR has treated the notion of "private life" as a broad concept, covering even aspects of professional life and public behaviour. It has also ruled that the protection of personal data is an important part of the right to respect for private life. However, despite the broad interpretation of private life, not all types of processing would per se compromise the rights protected under Article 8.

Where the ECtHR considers that the processing operation at stake affects the individuals' right to respect for private life, it will examine whether the interference is justified. The right to respect for private life is not an absolute right, but must be balanced against, and reconciled with, other legitimate interests and rights, be they of other persons (private interests) or of society as a whole (public interests).

The cumulative conditions under which an interference could be justified are:

In accordance with the law

According to the case law of the ECtHR, an interference is in accordance with the law if it is based on a provision of domestic law that has certain qualities. The law must be "accessible to the persons concerned and foreseeable as to its effects".[43] A rule is foreseeable "if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct".[44] Furthermore, "[t]he

42 ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 8 December 2008, para. 67.

43 ECtHR, *Amann v. Switzerland* [GC], No. 27798/95, 16 February 2000, para. 50; see also ECtHR, *Kopp v. Switzerland*, No. 23224/94, 25 March 1998, para. 55 and ECtHR, *Iordachi and Others v. Moldova*, No. 25198/02, 10 February 2009, para. 50.

44 ECtHR, *Amann v. Switzerland* [GC], No. 27798/95, 16 February 2000, para. 56; see also ECtHR, *Malone v. the United Kingdom*, No. 8691/79, 2 August 1984, para. 66; ECtHR, *Silver and Others v. the United Kingdom*, Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 March 1983, para. 88.

degree of precision required of 'the law' in this connection will depend on the particular subject-matter".[45]

Examples: In *Rotaru v. Romania*,[46] the applicant alleged a violation of his right to respect for his private life on account of the Romanian Intelligence Service's holding and use of a file containing his personal information. The ECtHR found that, while the domestic law allowed for the gathering, recording and archiving in secret files of information affecting national security, it did not lay down any limits on the exercise of those powers, which remained at the discretion of the authorities. For example, domestic law did not define the type of information that could be processed, the categories of people against whom surveillance measures could be taken, the circumstances in which such measures could be taken or the procedure to be followed. The Court therefore concluded that the domestic law did not comply with the requirement of foreseeability under Article 8 of the ECHR and that this article had been violated.

In *Taylor-Sabori v. the United Kingdom*,[47] the applicant had been the target of police surveillance. Using a 'clone' of the applicant's pager, the police were able to intercept messages sent to him. The applicant was arrested and charged with conspiracy to supply a controlled drug. Part of the prosecution's case against him consisted of the contemporaneous written notes of the pager messages, which the police had transcribed. However, at the time of the applicant's trial, there was no provision in British law governing the interception of communications transmitted via a private telecommunications system. The interference with his rights had therefore not been "in accordance with the law". The ECtHR concluded that this violated Article 8 of the ECHR.

45 ECtHR, *The Sunday Times v. the United Kingdom*, No. 6538/74, 26 April 1979, para. 49; see also ECtHR, *Silver and Others v. the United Kingdom*, Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 March 1983, para. 88.

46 ECtHR, *Rotaru v. Romania* [GC], No. 28341/95, 4 May 2000, para. 57; see also ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, No. 62540/00, 28 June 2007; ECtHR, *Shimovolos v. Russia*, No. 30194/09, 21 June 2011; and ECtHR, *Vetter v. France*, No. 59842/00, 31 May 2005.

47 ECtHR, *Taylor-Sabori v. the United Kingdom*, No. 47114/99, 22 October 2002.

Vukota-Bojić v. Switzerland[48] concerned secret surveillance of a social insurance claimant by private investigators commissioned by her insurance company. The ECtHR held that, while the surveillance measure at issue in the complaint had been ordered by a private insurance company, that company had been given the right by the State to provide benefits arising from compulsory medical insurance and to collect insurance premiums. A State could not absolve itself from responsibility under the convention by delegating its obligations to private bodies or individuals. Domestic law had to provide sufficient safeguards against abuse for interference with the rights under Article 8 of the ECHR to be "in accordance with the law". In the case at hand, the ECtHR concluded that there had been a violation of Article 8 of the ECHR because domestic law had failed to indicate with sufficient clarity the scope and manner of exercise of the discretion conferred on insurance companies acting as public authorities in insurance disputes to conduct secret surveillance of an insured person. In particular, it did not include sufficient safeguards against abuse.

Pursuing a legitimate aim

The legitimate aim may be either one of the named public interests or protection of the rights and freedoms of others. Legitimate aims that could justify an interference are, pursuant to Article 8 (2) of the ECHR, the interests of national security, public safety or the economic well-being of a country, the prevention of disorder or crime, the protection of health or morals, and the protection of rights and freedoms of other persons.

Example: In *Peck v. the United Kingdom*,[49] the applicant attempted suicide on the street by cutting his wrists, unaware that a CCTV camera was filming him. The police, who were watching the CCTV cameras, rescued him and subsequently passed the CCTV footage to the media, which published it without masking the applicant's face. The ECtHR found that there were no relevant or sufficient reasons that would justify the direct disclosure of the footage by the authorities to the public without having obtained the applicant's consent or masking his identity. The Court concluded that there had been a violation of Article 8 of the ECHR.

48 ECtHR, *Vukota-Bojić v. Switzerland*, No. 61838/10, 18 October 2016, para. 77.

49 ECtHR, *Peck v. the United Kingdom*, No. 44647/98, 28 January 2003, para. 85.

Necessary in a democratic society

The ECtHR has stated that "the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued".[50] When assessing whether a measure is necessary to address a pressing social need, the ECtHR examines its relevance and suitability in relation to the pursued aim. To this end, it may take into consideration whether the interference tries to address an issue which, if not addressed, could have a detrimental effect on society, whether there is evidence that the interference may mitigate such detrimental effect, and what the broader societal views on the issue at stake are.[51] For instance, the collection and storing of personal data by security services of particular individuals found to have links with terrorist movements would be an interference with the individuals' right to respect for private life, which nevertheless serves a serious, pressing social need: national security and the fight against terrorism. To meet the necessity test, the interference will also have to be proportionate. In the case law of the ECtHR, proportionality is addressed within the concept of necessity. Proportionality requires that an interference with the rights protected under the ECHR should not go any further than what is needed to fulfil the legitimate aim pursued. Important factors to take into account when performing the proportionality test is the scope of the interference, notably the number of persons affected, and the safeguards or caveats put in place to limit its scope or detrimental effects on the rights of individuals.[52]

Example: In *Khelili v. Switzerland*,[53] during a police check the police found the applicant to be carrying calling cards which read: "Nice, pretty woman, late thirties, would like to meet a man to have a drink together or go out from time to time. Tel. no. [...]". The applicant alleged that, following that discovery, the police entered her name in their records as a prostitute, an occupation which she consistently denied. The applicant requested that the word 'prostitute' be deleted from the police computer records. The ECtHR acknowledged in principle that retaining an individual's personal data on the ground that that person might commit another offence may under

50 ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987, para. 58.

51 Article 29 Data Protection Working Party (Article 29 Working Party) (2014), *Opinion on the application of the necessity and proportionality concepts and data protection within the law enforcement sector*, WP 211, Brussels, 27 February 2014, pp. 7–8.

52 *Ibid.*, pp. 9–11.

53 ECtHR, *Khelili v. Switzerland*, No. 16188/07, 18 October 2011.

certain circumstances be proportionate. However, in the applicant's case, the allegation of unlawful prostitution appeared too vague and general, was not supported by concrete facts since she had never been convicted of unlawful prostitution, and could therefore not be considered to meet a 'pressing social need' within the meaning of Article 8 of the ECHR. Regarding it as a matter for the authorities to prove the accuracy of the data stored on the applicant, and to the seriousness of the interference with the applicant's rights, the Court ruled that retention of the word 'prostitute' in the police files for years had not been necessary in a democratic society. The Court concluded that there had been a violation of Article 8 of the ECHR.

Example: In *S. and Marper v. the United Kingdom*,[54] the two applicants were arrested and charged with criminal offences. The police took their fingerprints and DNA samples, as provided for under the Police and Criminal Evidence Act. The applicants were never convicted of the offences: one was acquitted in court, and the criminal proceedings against the second applicant were discontinued. Nonetheless, their fingerprints, DNA profiles and cellular samples were kept and stored by the police in a database, and national legislation authorised their retention without an applicable time limit. While the United Kingdom argued that the retention assisted in the identification of future offenders, and thus pursued the legitimate aim of crime prevention and detection, the ECtHR considered the interference with the applicants' right to respect for private life to be unjustified. It recalled that the core principles of data protection require the retention of personal data to be proportionate in relation to the collection purpose and that retention periods must be limited. The Court accepted that extending the database to include DNA profiles not only of convicted persons, but also of all individuals who were suspected but not convicted, could have contributed to the detection and prevention of crime in the United Kingdom. However, it was "struck by the blanket and indiscriminate nature of the power of retention".[55]

Given the wealth of genetic and health information contained in the cellular samples, the interference with the applicants' right to private life was particularly intrusive. Fingerprints and samples could be taken from arrested persons, and retained indefinitely in the police database, irrespective of the nature and gravity of the offence, and even for minor offences not punishable

54 ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008.

55 *Ibid*., para. 119.

by imprisonment. Moreover, the possibilities for acquitted individuals to have their data removed from the database were limited. Finally, the ECtHR gave special consideration to the fact that one applicant was eleven years old when arrested. Retaining the personal data of a minor who is not convicted may be especially harmful given their vulnerability and the importance of their development and integration in society.[56] The Court held, unanimously, that the retention constituted a disproportionate interference with the right to private life that could not be regarded as necessary in a democratic society.

Example: In *Leander v. Sweden*,[57] the ECtHR ruled that the secret scrutiny of people applying for employment in posts of importance for national security was not, in itself, contrary to the requirement of being necessary in a democratic society. The special safeguards laid down in national law for protecting the interests of the data subject – for example, controls exercised by parliament and the Chancellor of Justice – resulted in the ECtHR's conclusion that the Swedish personnel control system met the requirements of Article 8 (2) of the ECHR. Having regard to the wide margin of appreciation available to it, the respondent state was entitled to consider that in the applicant's case the interests of national security prevailed over the individual ones. The Court concluded that there had not been a violation of Article 8 of the ECHR.

1.2.2. Conditions for lawful limitations under the EU Charter of Fundamental Rights

The structure and wording of the Charter is different than that of the ECHR. The Charter does not use the notion of interferences with guaranteed rights, but contains a provision on limitation(s) on the exercise of the rights and freedoms recognised by the Charter.

According to Article 52 (1), limitations on the exercise of the rights and freedoms recognised by the Charter and, accordingly, on the exercise of the right to the protection of personal data, are admissible only if they:

- are provided for by law; and

56 *Ibid.*, para. 124.

57 ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987, paras. 59 and 67.

- respect the essence of the right to data protection; and
- subject to the principle of proportionality, are necessary;[58] and
- meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

As personal data protection is a distinct and stand-alone fundamental right in the EU legal order, protected under Article 8 of the Charter, any processing of personal data by itself constitutes an interference with this right. It is immaterial whether the personal data in question relate to an individual's private life, are sensitive, or whether the data subjects have been inconvenienced in any way. To be lawful, the interference has to comply with all the conditions listed in Article 52 (1) of the Charter.

Provided for by law

Limitations on the right to personal data protection must be provided for by law. This requirement implies that limitations must be based on a legal basis that is adequately accessible and foreseeable and formulated with sufficient precision to enable individuals to understand their obligations and regulate their conduct. The legal basis must also clearly define the scope and manner of the exercise of the power by the competent authorities to protect individuals against arbitrary interference. This interpretation resembles the requirement for "lawful interference" under the ECtHR case law,[59] and it has been argued that the meaning of the expression "provided for by law" used in the Charter should be the same as that ascribed to it in connection with the ECHR.[60] The case law of the ECtHR, and especially the concept of "quality of the law" it has developed throughout the years, is a relevant consideration to be taken into account by the CJEU when interpreting the scope of Article 52 (1) of the Charter.[61]

58 On assessing the necessity of measures limiting the fundamental right to the protection of personal data, see: EDPS (2017), *Necessity Toolkit*, Brussels, 11 April 2017.

59 EDPS (2017), *Necessity Toolkit*, Brussels, 11 April 2017, p. 4; see also CJEU, *Opinion 1/15 of the Court (Grand Chamber)*, 26 July 2017.

60 CJEU, Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis, Opinion of Advocate General Saugmandsgaard Øe*, delivered on 19 July 2016, para. 140.

61 CJEU, C-70/10, *Scarlet Extended SA v. Société belge des auteurs compositeurs et éditeurs (SABAM), Opinion of Advocate General Cruz Villalón*, delivered on 14 April 2011, para. 100.

Respect the essence of the right

In the EU legal order, any limitation on the fundamental rights protected under the Charter must respect the essence of those rights. This means that limitations that are so extensive and intrusive so as to devoid a fundamental right of its basic content cannot be justified. If the essence of the right is compromised, the limitation must be considered unlawful, without a need to further assess whether it serves an objective of general interest and satisfies the necessity and proportionality criteria.

Example: The *Schrems* case[62] concerned the protection of individuals regarding the transfer of their personal data to third countries – in this case, the United States. Schrems, an Austrian citizen who had been a Facebook user for several years, lodged a complaint with the Irish data protection supervisory authority to denounce the transfer of his personal data from Facebook's Irish subsidiary to Facebook Inc. and the servers located in the US, where they were processed. He argued that, in light of the 2013 revelations by Edward Snowden, an American whistleblower, concerning the surveillance activities of US surveillance services, the law and practice of the US did not offer sufficient protection to personal data transferred to US territory. Snowden had revealed that the National Security Agency tapped directly into the servers of firms, such as Facebook, and could read the content of chats and private messages.

Transfers of data to the US were based on a Commission adequacy decision, adopted in 2000, allowing transfers to US companies that self-certified that they would protect personal data transferred from the EU and would comply with the so-called "Safe Harbour principles". When the case was brought before the CJEU, it examined the validity of the Commission decision in light of the Charter. It recalled that fundamental rights protection in the EU requires derogations and limitations to those rights to apply only in so far as strictly necessary. The CJEU regarded legislation permitting public authorities to access, on a general basis, the content of electronic communications as "compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter". The right would be rendered meaningless if US public authorities were authorised to access communications on a casual basis, without any objective justification based

62 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 6 October 2015.

on concrete considerations of national security or crime prevention that are specific individual concerned, and without those surveillance practices being accompanied by appropriate safeguards against abuse of power.

Moreover, the CJEU observed that "legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data" is incompatible with the fundamental right to effective judicial protection (Article 47 of the Charter). Thus, the Safe Harbour Decision failed to ensure a level of fundamental rights protection by the US essentially equivalent to that guaranteed within the EU under the directive read in the light of the Charter. The CJEU consequently invalidated the decision.[63]

Example: In *Digital Rights Ireland*,[64] the CJEU examined the compatibility of Directive 2006/24/EC (Data Retention Directive) with Articles 7 and 8 of the Charter. The directive obliged electronic communication service providers to retain traffic and location data for at least six months and up to 24 months, and to allow competent national authorities access to those data for the purpose of preventing, investigating, detecting and prosecuting serious crime. The directive did not permit retention of the content of the electronic communications. The CJEU noted that the data the providers had to retain pursuant to the directive included data necessary to trace and identify the source and destination of a communication, the date, time and duration of a communication, the calling number, numbers called, and IP addresses. Those data, "taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them".

63 The CJEU decision to invalidate Commission Decision 520/2000/EC was also based on other grounds that will be examined in other sections of this handbook. Notably, the CJEU considered that the decision unlawfully restricted the powers of national data protection supervisory authorities. In addition, under the Safe Harbour regime, there were no judicial remedies available for individuals in case they wished to access the personal data concerning them and/or obtain their rectification or deletion. Thus, the essence of the fundamental right to effective judicial protection, enshrined in Article 47 of the Charter, was also compromised.

64 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [GC], 8 April 2014.

Thus, the retention of personal data under the directive constituted a particularly serious interference with the rights to privacy and to personal data protection. However, the CJEU held that the interference did not adversely affect the essence of those rights. Concerning the right to privacy, its essence was not compromised because the directive did not permit the acquisition of knowledge of the content of the electronic communications as such. Similarly, the essence of the right to personal data protection was not compromised, as the directive required electronic communications services providers to respect certain principles of data protection and data security and to implement appropriate technical and organisational measures to this end.

Necessity and proportionality

Article 52 (1) of the Charter provides that, subject to the principle of proportionality, limitations on the exercise of the fundamental rights and freedoms recognised by the Charter may be made only if they are necessary.

A limitation may be **necessary** if there is a need to adopt measures for the public interest objective pursued – but necessity, as interpreted by the CJEU, also implies that the measures adopted must be less intrusive compared to other options for achieving the same goal. For limitations on the rights to respect for private life and protection of personal data, the CJEU applies a strict necessity test, holding that "derogations and limitations must apply only in so far as strictly necessary". If a limitation is deemed to be strictly necessary, there is also a need to assess whether it is proportionate.

Proportionality means that the advantages resulting from the limitation should outweigh the disadvantages the latter causes on the exercise of the fundamental rights at stake.[65] To reduce disadvantages and risks to the enjoyment of the rights to privacy and data protection, it is important that limitations contain appropriate safeguards.

65 EDPS (2017), *Necessity Toolkit*, p. 5.

Example: In *Volker und Markus Schecke*,[66] the CJEU concluded that by imposing an obligation to publish personal data relating to each natural person who was a beneficiary of aid from certain agricultural funds without drawing a distinction based on relevant criteria, such as the periods during which those persons received such aid, the frequency of such aid or the nature and amount thereof, the Council and the Commission had exceeded the limits imposed by the principle of proportionality.

Therefore, the CJEU found it necessary to declare invalid certain provisions of Council Regulation (EC) No. 1290/2005 and to declare Regulation No. 259/2008 invalid in its entirety.[67]

Example: In *Digital Rights Ireland,*[68] the CJEU held that the interference with the right to privacy caused by the Data Retention Directive did not compromise the essence of that right as it prohibited retention of the content of electronic communications. However, it concluded that the directive was incompatible with Article 7 and 8 of the Charter, and declared it invalid. Because traffic and location data, aggregated and taken as a whole, could be analysed and depict a detailed picture of individuals' private lives, it constituted a serious interference with these rights. The CJEU took into consideration that the directive required the retention of all metadata concerning fixed telephony, mobile telephony, internet access, internet email and internet telephony, applying to all means of electronic communication – the use of which is very widespread in people's everyday lives. Practically, it constituted an interference that affected the entire European population. Considering the extent and seriousness of this interference, traffic and location data retention could, according to the CJEU, be justified only for the purpose of fighting serious crime. In addition, the directive did not lay down any objective criteria that would ensure that access of the competent national authorities to the retained data is limited to what is strictly necessary.

66 CJEU, Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 9 November 2010, paras. 89 and 86.

67 Council Regulation (EC) No. 1290/2005 of 21 June 2005 on the financing of the common agricultural policy, OJ 2005 L 209; Commission Regulation (EC) No. 259/2008 of 18 March 2008 laying down detailed rules for the application of Council Regulation (EC) No. 1290/2005 as regards the publication of information on the beneficiaries of funds deriving from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD), OJ 2008 L 76.

68 CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [GC], 8 April 2014, para. 39.

Moreover, it did not contain substantive and procedural conditions governing the access and use of the retained data by national authorities, which were not made dependent on a prior review by a court or other independent body.

The CJEU came to a similar conclusion in the joined cases *Tele2 Sverige AB v. Post- och telestryrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others*.[69] These concerned the retention of traffic and location data of "all subscribers and registered users and all means of electronic communication as well as metadata" without "differentiation, limitation or exception according to the objective pursued".[70] In the case at hand, whether or not a person was linked, directly or indirectly, to serious criminal offences, or whether or not his or her communications were relevant for national security, was not a condition to have their data retained. In view of the absence of either a required link between the retained data and a threat to public security or time period or geographical area restrictions, the CJEU concluded that the national legislation exceeded the limits of what was strictly necessary for the purpose of fighting against serious crime.[71]

A similar approach, as regards necessity, is taken by the European Data Protection Supervisor in its *Necessity Toolkit*.[72] The toolkit aims to help assessment of compliance of proposed measures with EU law on data protection. It was developed to better equip EU policymakers and legislators responsible for preparing or scrutinising measures that involve processing of personal data and limit the right to personal data protection and other rights and freedoms laid down in the Charter.

Objectives of general interest

To be justified, any limitation on the exercise of the rights recognised by the Charter must also genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of other persons. Concerning the need to protect the rights and freedoms of others, the right to protection of personal data often interacts with other fundamental rights. Section 1.3 provides a detailed analysis of such interactions. As to objectives of general interest, these

69 CJEU, Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestryrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others* [GC], 21 December 2016, para. 105–106.

70 *Ibid.*, para. 105.

71 *Ibid.*, para. 107.

72 EDPS (2017), *Necessity Toolkit*, Brussels, 11 April 2017.

include the general objectives of the EU affirmed in Article 3 of the Treaty on the European Union (TEU), such as the promotion of peace and of the well-being of its peoples, social justice and protection and the establishment of an area of freedom, security and justice in which free movement of persons is ensured, in conjunction with appropriate measures to prevent and combat crime, as well as other objectives and interests protected by specific provisions of the treaties.[73] The General Data Protection Regulation further specifies Article 52 (1) of the Charter in this regard: Article 23 (1) of the regulation lists a series of objectives of general interest considered legitimate for limiting the rights of individuals, provided that the limitation respects the essence of the right to personal data protection and is necessary and proportionate. National security and defence, crime prevention, the protection of important economic and financial interests of the EU or Member States, public health and social security are among the public interest aims mentioned therein.

It is important to define and explain the objective of general interest pursued by the limitation in sufficient detail, as the necessity of the limitation will be assessed against that background. A clear, detailed description of the objective of the limitation and the measures proposed is essential to allow the assessment as to whether it is necessary.[74] The objective pursued, and necessity and proportionality of the limitation are closely linked.

Example: *Schwarz v. Stadt Bochum*[75] concerned limitations on the right to respect for private life and the right to personal data protection arising from the taking and storing of fingerprints when Member State authorities issue passports.[76] The applicant applied to Stadt Bochum for a passport, but refused to have his fingerprints taken; following this, the Stadt Bochum refused his passport application. He then brought an action before a German court to have a passport issued without this fingerprints being taken. The German court referred the issue to the CJEU, asking whether Article 1 (2) of Regulation 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States is to be considered valid.

73 Explanations relating to the Charter of Fundamental Rights (2007/C 303/02), OJ 2007 No. C 303, pp. 17–35.

74 EDPS (2017), *Necessity Toolkit*, Brussels, 11 April 2017, p. 4.

75 CJEU, C-291/12, *Michael Schwarz v. Stadt Bochum*, 17 October 2013.

76 *Ibid.*, paras. 33–36.

The CJEU pointed out that fingerprints **constitute personal data**, as they objectively contain unique information about individuals that allows them to be identified with precision, while taking and storing fingerprints constitute processing. The latter processing, which is governed by Article 1 (2) of Regulation No. 2252/2004, constitutes a threat to the rights to respect for private life and personal data protection.[77] However, Article 52 (1) of the Charter allows for limitations on the exercise of those rights, so long as these limitations are provided for by law, respect the essence of those rights and, in accordance with the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

In the present case, the CJEU first noted that the limitation arising from the taking and storing of fingerprints when issuing passports must be considered to be **provided for by law** since those operations are provided for by Article 1 (2) of Regulation No. 2252/2004. Second, the latter regulation was designed to prevent the falsification of passports and their fraudulent use. Thus, Article 1 (2) is in place to prevent, among others, illegal entry into the EU, and so pursues an objective of general interest recognised by the Union. Third, it was not apparent from the evidence available to the CJEU, nor had it been claimed, that the limitations placed on the exercise of these rights in the present case did not respect the essence of those rights. Fourth, the storage of fingerprints on a highly secure storage medium as provided for by that provision requires sophisticated technology. Such storage is likely to reduce the risk of passports being falsified and to facilitate the work of the authorities responsible for checking the authenticity of passports at EU borders. The fact that the method is not wholly reliable is not decisive. Although the method does not prevent all unauthorised persons from being accepted, it is enough that it significantly reduces the likelihood of such acceptance. In light of the foregoing, the CJEU found that the taking and storing of fingerprints referred to in Article 1 (2) of Regulation No. 2252/2004 were appropriate for attaining the aims pursued by that regulation and, by extension, the objective of preventing illegal entry to the EU.[78]

The CJEU next assessed whether such processing is **necessary**, noting that the action at issue involved no more than the taking of prints of two fingers,

77 *Ibid.*, paras. 27–30.

78 *Ibid.*, paras. 35–45.

which can, moreover, generally be seen by others, so that this is not an operation of an intimate nature. Nor does it cause any particular physical or mental discomfort to the person affected any more than when that person's facial image is taken. It should also be noted that the only real alternative to the taking of fingerprints raised in the course of the proceedings before the CJEU was an iris scan. Nothing in the case file submitted to the CJEU suggested that the latter procedure would interfere less with the rights recognised by Articles 7 and 8 of the Charter than the taking of fingerprints. Furthermore, with regard to the effectiveness of those two methods, it is common ground that iris-recognition technology is not yet as advanced as fingerprint-recognition technology, is currently significantly more expensive than the procedure for comparing fingerprints and is, for that reason, less suitable for general use. Accordingly, the CJEU had not been made aware of any measures that would be both sufficiently effective in helping to achieve the aim of protecting against the fraudulent use of passports and less of a threat to the rights recognised by Articles 7 and 8 of the Charter than the measures deriving from the method based on the use of fingerprints.[79]

The CJEU noted that Article 4 (3) of Regulation No. 2252/2004 explicitly states that fingerprints may be used only for verifying the authenticity of a passport and the identity of its holder, while Article 1 (2) of the regulation does not provide for the storage of fingerprints except within the passport itself, which belongs to the holder alone. Thus, the regulation did not provide a legal basis for the centralised storage of data collected thereunder or for the use of such data for purposes other than that of preventing illegal entry into the EU.[80] In light of all the foregoing considerations, the CJEU concluded that the examination of the referred question revealed nothing capable of affecting the validity of Article 1 (2) of Regulation No. 2252/2004.

Relationship between the Charter and the ECHR

Despite involving different wording, conditions for lawful limitations on the rights in Article 52 (1) of the Charter are reminiscent of Article 8 (2) of the ECHR concerning the right to respect for private life. In their case law, the CJEU and the ECtHR often refer to each other's judgments, as part of the constant dialogue between the two courts to seek a harmonious interpretation of data protection rules. Article 52 (3) of

79 CJEU, C-291/12, *Michael Schwarz v. Stadt Bochum*, 17 October 2013, paras. 46–53.

80 *Ibid.*, paras. 56–61.

the Charter states that, "in so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention". However, Article 8 of the Charter does not directly correspond to an article in the ECHR.[81] Article 52 (3) of the Charter concerns the content and scope of the rights protected by each legal order, rather than the conditions for their limitation. However, in view of the wider context of dialogue and cooperation between the two courts, the CJEU may take into account in its analyses the criteria for lawful limitation under Article 8 of the ECHR, as interpreted by the ECtHR. The opposite scenario, by which the ECtHR may refer to the conditions for lawful limitation under the Charter, is also possible. In any case, it should also be taken into account that there is no perfect equivalent of Article 8 of the Charter in the ECHR that refers to the protection of personal data, and notably to the rights of the data subject, the legitimate grounds for processing and the supervision by an independent authority. Some components of Article 8 of the Charter can be founded in the ECtHR case law developed under Article 8 of the ECHR and relating to Convention 108.[82] This link ensures the existence of mutual inspiration between the CJEU and the ECtHR on matters related to data protection.

1.3. Interaction with other rights and legitimate interests

Key points

- The right to data protection often interacts with other rights, such as freedom of expression and the right to receive and impart information.
- This interaction is often ambivalent: while there are situations where the right to personal data protection is in tension with a specific right, there are also situations where the right to personal data protection effectively ensures the respect of the same specific right. For instance, this is the case for freedom of expression, given that professional secrecy is a component of the right to respect for private life.
- The need to protect the rights and freedoms of others is one of the criteria used to assess the lawful limitation of the right to personal data protection.

81 EDPS (2017), *Necessity Toolkit*, Brussels, 11 April 2017, p. 6.

82 Explanations relating to the European Charter of Fundamental Rights (2007/C 303/02), Art. 8.

- When different rights are at stake, courts must carry out a balancing exercise to reconcile them.
- The General Data Protection Regulation requires Member States to reconcile the right to personal data protection with freedom of expression and information.
- Member States may also adopt specific rules in national law to reconcile the right to personal data protection with public access to official documents and obligations of professional secrecy.

The right to personal data protection is not an absolute right; the conditions for the lawful limitation of this right have been detailed above. One of the criteria for lawful limitations on rights, recognised both under CoE and EU law, is that the interference with data protection is necessary for the protection of the rights and freedoms of others. Where data protection interacts with other rights, both the ECtHR and the CJEU have repeatedly stated that a balancing exercise with other rights is necessary when applying and interpreting Article 8 of the ECHR and Article 8 of the Charter.[83] Several important examples will illustrate how this balance is reached.

In addition to the balancing exercise carried out by these courts, states may, if necessary, adopt legislation to reconcile the right to personal data protection with other rights. For this reason, the General Data Protection Regulation provides a number of areas of national derogation.

With respect to freedom of expression, the GDPR requires Member States to reconcile, by law, "the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression".[84] Member States can also adopt laws to reconcile data protection with public access to official documents and obligations of professional secrecy protected as a form of the right to respect for private life.[85]

83 ECtHR, *Von Hannover v. Germany (No. 2)* [GC], Nos. 40660/08 and 60641/08, 7 February 2012; CJEU, Joined cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 November 2011, para. 48; CJEU, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [GC], 29 January 2008, para. 68.

84 General Data Protection Regulation, Art. 85.

85 *Ibid.*, Art. 86 and 90.

1.3.1. Freedom of expression

One of the rights that interacts most significantly with the right to data protection is the right to freedom of expression.

Freedom of expression is protected by Article 11 of the Charter ('Freedom of expression and information'). This right includes the "freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers". Freedom of information, according to both Article 11 of the Charter and Article 10 of the ECHR, protects the right not only to impart but also to *receive* information.

Limitations on the freedom of expression must comply with the criteria provided for in Article 52 (1) of the Charter, described above. Additionally, Article 11 corresponds to Article 10 of the ECHR. Pursuant to Article 52 (3) of the Charter, insofar as it contains rights that correspond to rights guaranteed by the ECHR, "the meaning and scope of those rights shall be the same as those laid down by the said Convention". The limitations that may lawfully be imposed on the right guaranteed by Article 11 of the Charter may therefore not exceed those provided for in Article 10 (2) of the ECHR – that is to say, they must be prescribed by law and be necessary in a democratic society "for the protection [...] of the reputation or rights of others". Such rights encompass, notably, the right to respect for private life and the right to personal data protection.

The relationship between the protection of personal data and freedom of expression is governed by Article 85 of the General Data Protection Regulation, entitled "Processing and freedom of expression and information". According to this article, Member States shall reconcile the right to personal data protection with the right to freedom of expression and information. In particular, exemptions and derogations from specific chapters of the General Data Protection Regulation shall be made for journalistic purposes or the purpose of academic, artistic or literary expression, insofar as they are necessary to reconcile the right to personal data protection with the freedom of expression and information.

Example: In *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*,[86] the CJEU was asked to define the relationship between

86 CJEU, C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [GC], 16 December 2008, paras. 56, 61 and 62.

data protection and freedom of the press.[87] It had to examine a company's dissemination, through an SMS service, of tax data on some 1.2 million natural persons lawfully obtained from the Finnish tax authorities. The Finish data protection supervisory authority had issued a decision requiring the company to stop disseminating these data. The company challenged this decision in a national court, which requested clarification from the CJEU on the interpretation of the Data Protection Directive. In particular, the CJEU had to verify whether the processing of personal data, which the tax authorities made available to allow mobile telephone users to receive tax data relating to other natural persons, must be considered as an activity carried out solely for journalistic purposes. After having concluded that the company's activities were 'processing of personal data' within the meaning of Article 3 (1) of the Data Protection Directive, the CJEU analysed Article 9 of the directive (on processing of personal data and freedom of expression). It first noted the importance of the right to freedom of expression in every democratic society and held that notions relating to that freedom, such as journalism, should be interpreted broadly. It then observed that, to achieve a balance between the two fundamental rights, the derogations and limitations of the right to data protection must apply only insofar as strictly necessary. In those circumstances, the CJEU held that activities such as those carried out by the companies at issue concerning data from documents that are in the public domain under national legislation may be classified as 'journalistic activities' if their object is the disclosure to the public of information, opinions or ideas, irrespective of the medium used to transmit them. It also ruled that these activities are not limited to media undertakings and may be undertaken for profit-making purposes. However, the CJEU left it to the national court to determine whether this was the case with the particular facts of this case.

The same case was also examined by the ECtHR, after the national court decided, based on the guidance from the CJEU, that the supervisory authority's order to discontinue publication of all tax information was a justified interference with the company's freedom of expression. The ECtHR upheld this approach.[88] It found that, even though there was an interference with the companies' right to

87 The case concerned the interpretation of the Data Protection Directive, Art. 9 – now replaced by Art. 85 of the General Data Protection Regulation – which read: "Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression".

88 ECtHR, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, No. 931/13, 27 June 2017.

impart information, the interference was in accordance with the law, pursued a legitimate aim and was necessary in a democratic society.

The Court recalled the case law criteria that should guide national authorities, and the ECtHR itself, when balancing freedom of expression with the right to respect for private life. Where political speech or a debate on a matter of public interest are at stake, there is little scope for restriction of the right to receive and impart information as the public has a right to be informed, "and this is an essential right in a democratic society".[89] However, press articles aiming solely to satisfy the curiosity of a particular readership regarding details of a person's private life cannot be deemed to contribute to a debate of public interest. The derogation from data protection rules for journalistic purposes is intended to allow journalists to access, collect and process data to be able to perform their journalistic activities. Thus, there was indeed a public interest in providing access to, and allowing the applicant companies to collect and process, the large amounts of taxation data at stake. By contrast, the Court found that there was no public interest in the bulk dissemination of such raw data by the newspapers, in unaltered form and without any analytical input. The information on taxation might have enabled curious members of the public to categorise individuals according to their economic status and satisfy the public's thirst for information about the private lives of others. This could not be regarded as contributing to a debate of public interest.

Example: In *Google Spain,*[90] the CJEU considered whether Google was obliged to delete outdated information about the applicant's financial difficulties from its search list results. When a search was undertaken on the Google search engine using the applicant's name, the results of the search provided links to old newspaper articles mentioning his connection with bankruptcy proceedings. The applicant considered this an infringement on his rights to respect for private life and for the protection of personal data, as the proceedings had been concluded years ago, making such references irrelevant.

The CJEU first clarified that internet search engines and search results providing personal data can establish a detailed profile of an individual. In light of an increasingly digitised society, the requirement for personal data

89 *Ibid.*, para. 169.

90 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 May 2014, paras. 81–83.

to be accurate and for its publication not to go beyond what is necessary, i.e. provide information to the public, is fundamental to ensuring a high level of data protection to individuals. The "controller in respect of that processing must ensure, within the framework of its responsibilities, powers and capabilities, that that processing meets the requirements" of EU law, in order that the legal guarantees established have full effect. This means that the right to have one's personal data erased when the processing is no longer necessary or outdated also covers search engines, which were found to be controllers, not merely processors (see Section 2.3.1).

On examining whether Google was required to remove the links related to the applicant, the CJEU held that, under certain conditions, individuals have the right to obtain erasure of their personal data from an internet search engine's search results. This right may be invoked where information relating to an individual is inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing. The CJEU acknowledged that this right is not absolute; it needs to be balanced with other rights, in particular the interest and right of the general public in having access to the information. Each request for erasure needs a case-by-case assessment to seek a balance between the fundamental rights to personal data protection and private life of the data subject on the one hand, and the legitimate interests of all internet users on the other. The CJEU provided guidance on the factors to take into consideration during the balancing exercise. The nature of the information in question is a particularly important factor. If information is sensitive to the private life of the individual, and where there is no public interest in the availability of the information, data protection and privacy would override the right of the general public to have access to the information. On the contrary, if it appears that the data subject is a public figure, or that the information is of such nature to justify granting the general public access to such information, then the interference with the fundamental rights to data protection and privacy is justified.

Following the judgment, the Article 29 Working Party adopted guidelines on the implementation of the CJEU ruling. The guidelines include a list of common criteria to be used by the supervisory authorities when handling complaints related to individuals' requests for deletion and to guide them in this balancing of rights exercise.[91]

91 Article 29 Working Party (2014), *Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, WP 225, Brussels, 26 November 2014.

Concerning the reconciliation of the right to data protection with the right to freedom of expression, the ECtHR has issued several landmark judgments.

Example: In *Axel Springer AG v. Germany*,[92] the ECtHR held that an injunction restraining the applicant company from publishing an article on the arrest and conviction of a well-known actor violated Article 10 of the ECHR. The ECtHR reiterated the criteria to be considered when balancing the right to freedom of expression against the right to respect for private life, as established in its case law:

- whether the event that the published article concerned was of general interest;
- whether the person concerned was a public figure; and
- how the information was obtained and whether it was reliable.

The ECtHR found that the actor's arrest and conviction was a public judicial fact and was therefore of public interest; that the actor was sufficiently well-known to qualify as a public figure; and that the information had been provided by the public prosecutor's office and its accuracy was not in dispute by the parties. Therefore, the publication restrictions imposed on the company had not been reasonably proportionate to the legitimate aim of protecting the applicant's private life. The Court concluded that there had been a violation of Article 10 of the ECHR.

Example: *Coudec and Hachette Filipacchi Associés v. France*[93] concerned the publication by a French weekly magazine of an interview with Ms Coste, who claimed that Prince Albert of Monaco was the father of her son. The interview also described the relationship of Ms Coste with the prince, and the manner in which he reacted to the birth of the child, accompanied by photos of the prince with the child. Prince Albert brought proceedings against the publishing company for violation of his right to protection of private life. The French courts held that the publication of the article had caused irreversible damage to Prince Albert and ordered the publisher to pay damages and to publish the details of the judgment on the magazine's front cover.

92 ECtHR, *Axel Springer AG v. Germany* [GC], No. 39954/08, 7 February 2012, paras. 90 and 91.

93 ECtHR, *Coudec and Hachette Filipacchi Associés v. France* [GC], No. 40454/07, 10 November 2015.

The publishers of the magazine brought the case before the ECtHR, claiming that the judgment of the French courts interfered unjustifiably with their right to freedom of expression. The ECtHR had to balance Prince Albert's right to respect for private life with the publisher's right of expression and the general public's right to have the information. The right of Ms Coste to share her story with the public and the child's interest in having the father-child relationship officially established were also important considerations.

The ECtHR held that publication of the interview constituted an interference with the prince's private life and went on to examine whether the interference was necessary. It considered that the publication concerned a public figure and a matter of public interest, as the citizens of Monaco had an interest in knowing about the existence of a child of the prince, as the future of a hereditary monarchy is "intrinsically linked to the existence of descendants" and thus a matter of concern for the public.[94] The Court also noted that the article had allowed Ms Coste and her child to exercise their right to freedom of expression. The domestic courts had failed to give due consideration to the principles and criteria developed through ECtHR case law for the balancing of the right to respect for private life and the right to freedom of expression. It concluded that France violated Article 10 of the ECHR on the freedom of expression.

In the ECtHR case law, one of the crucial criteria regarding the balancing of these rights is whether or not the expression in question contributes to a debate of general public interest.

Example: In *Mosley v. the United Kingdom*,[95] a national weekly newspaper published intimate photographs of the applicant, a well-known figure who subsequently successfully brought a civil claim against the publisher and was awarded damages. Despite the monetary compensation awarded, he complained that he remained a victim of a violation of his right to privacy as he had been denied the opportunity to seek an injunction before the publication of the photos in question owing to the absence of any legal requirement for the newspaper to give advance notice of publication.

94 *Ibid*., paras. 104–116.

95 ECtHR, *Mosley v. the United Kingdom*, No. 48009/08, 10 May 2011, paras. 129 and 130.

The ECtHR noted that, although the dissemination of such material was generally for the purposes of entertainment rather than education, it undoubtedly benefited from the protection of Article 10 of the ECHR, which might yield to the requirements of Article 8 of the ECHR where the information was of a private and intimate nature and there was no public interest in its dissemination. However, particular care had to be taken when examining constraints which might operate as a form of censorship prior to publication. In light of the chilling effect to which a pre-notification requirement might give rise, the doubts about its effectiveness, and the wide margin of appreciation in that area, the ECtHR concluded that the existence of a legally binding pre-notification requirement was not required under Article 8. Accordingly, the Court concluded that there had been no violation of Article 8.

Example: In *Bohlen v. Germany*,[96] the applicant, a well-known singer and artistic producer, had published an autobiographical book and subsequently been forced to remove some passages following court rulings. The story was widely covered in national media, and a tobacco company launched a humorous advertising campaign referring to this event, using the applicant's first name without his consent. The applicant unsuccessfully sought damages from the advertising company, alleging a violation of his rights under Article 8 of the ECHR. The ECtHR reiterated the criteria that guide the balancing between the right to respect for private life and the right to freedom of expression and held that there was no violation of Article 8. The applicant was a public figure and the advertisement did not refer to the details of his private life, but to a public event that had already been covered by the media and formed part of a public debate. In addition, the advertisement was of a humorous nature and did not contain anything degrading or negative regarding the applicant.

Example: In *Biriuk v. Lithuania*,[97] the applicant argued before the ECtHR that Lithuania had failed to fulfil its obligation to secure respect of her right to private life, because even though a serious violation of her privacy had been committed by a major newspaper, she was awarded a derisory sum of pecuniary damages by the national courts examining the case. When awarding the non-pecuniary damages, national courts had applied

96 ECtHR, *Bohlen v. Germany*, No. 53495/09, 19 February 2015, paras. 45–60.

97 ECtHR, *Biriuk v. Lithuania*, No. 23373/03, 25 November 2008.

the provisions of the national law on the provision of information to the public, which imposed a low ceiling on compensation for non-pecuniary damage caused by the unlawful dissemination to the public by the media of information about a person's private life. The case stemmed from the biggest Lithuanian daily newspaper's publication of a front page article reporting that the applicant was HIV positive. The article also criticised the applicant's behaviour and questioned her moral standards.

The ECtHR recalled that the protection of personal data, not least medical data, is of fundamental importance to the right to respect of private life under the ECHR. The confidentiality of health data is particularly important, since disclosure of medical data (the HIV status of the applicant in this case) may dramatically affect a person's private and family life, his or her employment situation, and inclusion in society. The Court attached particular significance to the fact that, according to the report in the newspaper, the hospital's medical staff had provided information about the applicant's HIV status in an evident breach of their obligation to medical secrecy. There had thus been no legitimate interference with the applicant's right to private life.

The article had been published by the press, and freedom of expression is also a fundamental right under the ECHR. However, when examining whether the existence of a public interest justified the publication of that type of information about the applicant, the Court found that the main purpose of the publication was to increase the newspaper's sales by satisfying reader curiosity. Such a purpose could not be deemed to contribute to any debate of general interest to society. As this was a case of "outrageous abuse of press freedom", the severe limitations in redressing the damage and the low sum of non-pecuniary damages provided under national law meant that Lithuania had failed to fulfil its positive obligation to protect the applicant's right to private life. The ECtHR found that there had been a violation of Article 8 of the ECHR.

The right to freedom of expression and the right to personal data protection are not always in conflict. There are instances where the effective protection of personal data guarantees freedom of expression.

Example: The CJEU in *Tele2 Sverige* stated that the interference caused by Directive 2006/24 (Data Retention Directive) with the fundamental rights laid down in Articles 7 and 8 of the Charter was "wide-ranging, and

it must be considered to be particularly serious. Furthermore…the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance". The CJEU also found that the generalised retention of traffic and location data could have an effect on the use of electronic communication and "consequently on the exercise by the users thereof of their freedom of expression guaranteed in Article 11 of the Charter".[98] In that sense, by requiring strict safeguards for data retention not to be carried out in a generalised manner, data protection rules ultimately contribute to the exercise of freedom of expression.

Concerning the right to receive information, which also forms part of freedom of expression, there is a growing realisation of the importance of government transparency for the functioning of a democratic society. Transparency is an objective of general interest that could thus justify an interference with the right to data protection, if necessary and proportionate, as explained in Section 1.2. In the past two decades, in consequence, the right to access documents held by public authorities has been acknowledged as an important right of every EU citizen, and any natural or legal person residing or having its registered office in a Member State.

Under CoE law, reference can be made to the principles enshrined in the Recommendation on access to official documents, which inspired the drafters of the Convention on Access to Official Documents (Convention 205).[99]

Under EU law, the right of access to documents is guaranteed by Regulation 1049/2001 regarding public access to European Parliament, Council and Commission documents (Access to Documents Regulation).[100] Article 42 of the Charter and Article 15 (3) of the TFEU have extended this right of access "to documents

98 CJEU, Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others* [GC], 21 December 2016, para. 37 and 101; CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [GC], 8 April 2014, para. 28.

99 Council of Europe, Committee of Ministers (2002), Recommendation Rec (81) 19 and Recommendation Rec (2002) 2 to member states on access to official documents, 21 February 2002; Council of Europe, Convention on Access to Official Documents, CETS No. 205, 18 June 2009. The Convention has not yet entered into force.

100 Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ 2001 L 145.

of the institutions, bodies, offices and agencies of the Union, regardless of their form".

This right may come into conflict with the right to data protection if access to a document would reveal others' personal data. Article 86 of the General Data Protection Regulation clearly provides that personal data in official documents held by public authorities and bodies may be disclosed by the authority or body concerned in accordance with Union[101] or Member State law to reconcile public access to official documents with the right to data protection pursuant to the regulation.

Requests for access to documents or information held by public authorities may therefore need balancing with the right to data protection of persons whose data are contained in the requested documents.

Example: In *Volker und Markus Schecke and Hartmut Eifert v. Land Hessen*,[102] the CJEU had to judge the proportionality of the publication, required by EU legislation, of the name of the beneficiaries of EU agricultural subsidies and the amounts they received. The publication aimed to enhance transparency and contribute to public control of the appropriate use of public funds by the administration. Several beneficiaries contested the proportionality of this publication.

The CJEU, noting that the right to data protection is not absolute, argued that the publication on a website of data naming the beneficiaries of two EU agricultural aid funds and the precise amounts received constitutes an interference with their private life, in general, and with the protection of their personal data, in particular.

The CJEU found that such interference with Articles 7 and 8 of the Charter was provided for by law and met an objective of general interest recognised by the EU – namely, enhancing the transparency of community funds use. However, the CJEU held that the publication of the names of natural persons who are beneficiaries of EU agricultural aid from these two funds and the exact amounts received constituted a disproportionate measure and was not justified having regard to Article 52 (1) of the Charter. It acknowledged the

101 Article 42 of the Charter, Article 15 (3) of the TFEU and Regulation 1049/2009.

102 CJEU, Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 9 November 2010, paras. 47–52, 58, 66–67, 75, 86 and 92.

importance, in a democratic society, of keeping taxpayers informed of the use of public funds. However, as "no automatic priority can be conferred on the objective of transparency over the right to protection of personal data",[103] EU institutions were obliged to balance the Union's interest in transparency with the limitation on the exercise of the rights to privacy and data protection that beneficiaries suffered as a result of the publication.

The CJEU considered that the EU institutions had not properly carried out this balancing exercise, since it was possible to envisage measures which would affect less adversely the fundamental rights of the individuals, while also effectively contributing to the transparency objective pursued by the publication. For instance, instead of a general publication affecting all beneficiaries, giving their name and the precise amounts received by each of them, a distinction could be drawn based on relevant criteria such as the periods during which those persons had received the aid, the frequency of the aid or its amount and nature.[104] The CJEU thus declared partially invalid the EU legislation on the publication of information relating to the beneficiaries of European agricultural funds.

Example: In *Rechnungshof v. Österreichischer Rundfunk and Others*,[105] the CJEU reviewed certain Austrian legislation's compatibility with EU data protection law. The legislation required a state body to collect and transmit data on income for purposes of publishing the name and income of employees of various public entities in an annual report made available to the general public. Some individuals refused to communicate their data on the ground of data protection.

In its opinion, the CJEU relied on the protection of fundamental rights as a general principle of EU law and on Article 8 of the ECHR, recalling that the Charter was not binding at that time. It held that the collection of data on an individual's professional income, and in particular its communication to third parties, falls within the scope of the right to respect for private life, and constitutes an infringement of this right. The interference could be justified if it had been in accordance with the law, pursued a legitimate aim and had

103 *Ibid.*, para. 85.

104 *Ibid.*, para. 89.

105 CJEU, C-465/00, C-138/01 and C-139/09, *Rechnungshof v. Österreichischer Rundfunk and Others and Christa Neukomm and Jospeh Lauermann v. Österreichischer Rundfunk*, 20 May 2003.

been necessary in a democratic society to achieve that aim. The CJEU noted that the Austrian legislation pursued a legitimate aim, as its objective was to keep salaries of public employees within reasonable limits – a consideration that is also related to the economic well-being of the country. However, Austria's interest in ensuring the best use of public funds had to be balanced against the seriousness of the interference with the right of the persons concerned to respect for their private life.

While leaving it to the national court to ascertain whether publication of the data on the income of individuals was necessary and proportionate to the aim pursued by the legislation, the CJEU called for the national court to examine whether such an aim could not have been achieved equally effectively by less intrusive means. An example would be the transmission of the personal data only to the monitoring public bodies and not to the general public.

In subsequent cases, it became evident that the balancing between data protection and access to documents requires a detailed, case-by-case analysis. Neither right can automatically overrule the other. The CJEU had the opportunity to interpret the right to access to documents containing personal data in two cases.

Example: In *European Commission v. Bavarian Lager*,[106] the CJEU defined the scope of personal data protection in the context of access to documents of EU institutions, and the relationship between Regulation No. 1049/2001 (Access to Documents Regulation) and Regulation No. 45/2001 (EU Institutions Data Protection Regulation). Bavarian Lager, established in 1992, imports bottled German beer into the United Kingdom, principally for public houses and bars. It encountered difficulties, however, because British legislation *de facto* favoured national producers. In response to Bavarian Lager's complaint, the European Commission instituted proceedings against the United Kingdom for failure to fulfil its obligations, which led it to amend the disputed provisions and align them with EU law. Bavarian Lager then asked the Commission, among other documents, for a copy of the minutes of a meeting attended by representatives of the Commission, the British authorities and the *Confédération des Brasseurs du Marché Commun* (CBMC). The Commission agreed to disclose certain documents relating to the meeting, but blanked out five names appearing in the minutes – two persons having expressly objected

106 CJEU, C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd.* [GC], 29 June 2010.

to the disclosure of their identity and the Commission having been unable to contact the three others. By decision of 18 March 2004, the Commission rejected a new Bavarian Lager application to obtain the full minutes of the meeting, citing in particular the protection of the private life of those persons, as guaranteed by the EU Institutions Data Protection Regulation.

Since it was not satisfied with this position, Bavarian Lager brought an action before the Court of First Instance. That court annulled the Commission decision by judgment of 8 November 2007 (case T-194/04, *The Bavarian Lager Co. Ltd v. Commission of the European Communities*), finding that the mere entry of the names of the persons in question on the list of persons attending a meeting on behalf of the body they represented did not undermine private life and did not place the private lives of those persons in any danger.

On appeal by the Commission, the CJEU annulled the Court of First Instance's judgment. The CJEU held that the Access to Documents Regulation establishes "a specific and reinforced system of protection of a person whose personal data could, in certain cases, be communicated to the public". According to the CJEU, where a request based on the Access to Documents Regulation thus seeks to obtain access to documents that include personal data, the provisions of the EU Institutions Data Protection Regulation become applicable in their entirety. The CJEU then concluded that the Commission was right to reject the application for access to the full minutes of the meeting of October 1996. In the absence of the consent of the five participants at that meeting, the Commission sufficiently complied with its duty of openness by releasing a version of the document in question with their names blanked out.

Moreover, according to the CJEU, "as Bavarian Lager has not provided any express and legitimate justification or any convincing argument in order to demonstrate the necessity for those personal data to be transferred, the Commission has not been able to weigh up the various interests of the parties concerned. Nor was it able to verify whether there was any reason to assume that the data subjects' legitimate interests might be prejudiced", as required by the EU Institutions Data Protection Regulation.

Example: In *Client Earth and PAN Europe v. EFSA*,[107] the CJEU examined whether the decision of the European Food and Safety Authority (EFSA)

107 CJEU, C-615/13P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (EFSA), European Commission*, 16 July 2015.

to refuse applicants full access to documents was necessary to protect the privacy and data protection rights of the persons to whom the documents referred. The documents concerned a draft guidance report prepared by an EFSA working group in collaboration with external experts, on the placement of plant protection products on the market. Initially, EFSA granted partial access to the applicants, denying access to some working versions of the draft guidance document. Subsequently, it granted access to the draft version that included the individual comments of the external experts. However, it redacted the names of the experts, invoking Article 4 (1) (b) of Regulation 45/2001 on the processing of personal data by EU institutions and bodies and the need to protect the privacy of the external experts. At first instance, the General Court of the EU upheld EFSA's decision.

On appeal by the applicants, the CJEU reversed the judgment of first instance. It concluded that the transfer of personal data in that case was necessary to ascertain the impartiality of each of the external experts in carrying out their tasks as scientists and to ensure that the decision-making process in EFSA remains transparent. According to the CJEU, EFSA did not specify how revealing the names of the external experts who had made specific comments on the draft guidance document would prejudice the experts' legitimate interests. A general argument that disclosure is likely to undermine privacy does not suffice if it is unsupported by evidence specific to each case.

According to these judgments, interference with the right to data protection in the context of access to documents needs a specific and justified reason. The right of access to documents cannot automatically overrule the right to data protection.[108]

This approach is similar to that of the ECtHR with regard to privacy and access to documents, as the following judgment demonstrates. In the *Magyar Helsinki* judgment, the ECtHR stated that Article 10 did not confer on the individual a right of access to information held by a public authority or oblige the government to impart such information to the individual. However, such a right or obligation could arise – firstly, where disclosure of the information is imposed by a judicial order that has gained legal force; secondly, where access to the information is instrumental for an individual's exercise of his or her right to freedom of expression – particularly the freedom to receive and impart information – and where its denial would interfere

108 See, however, the detailed deliberations in EDPS (2011), *Public access to documents containing personal data after the Bavarian Lager ruling*, Brussels, 24 March 2011.

with that right.[109] Whether, and to which extent, the denial of access to information constitutes an interference with an applicant's freedom of expression has to be assessed in each individual case and in light of its particular circumstances, including: (i) the purpose of the information request; (ii) the nature of the information sought; (iii) the role of the applicant; and (iv) whether the information was ready and available.

Example: In *Magyar Helsinki Bizottság v. Hungary,*[110] the applicant, a human rights NGO, requested information from the police relating to the work of *ex officio* defence counsel, to complete a study on the functioning of the public defenders' system in Hungary. The police refused to provide the information, arguing that it constituted personal data not subject to disclosure. Applying the above criteria, the ECtHR held that there had been an interference with a right protected under Article 10. More precisely, the applicant wished to exercise the right to impart information on a matter of public interest, had sought access to information to that end, and the information was necessary for the exercise of the applicant's right to freedom of expression. The information on the appointment of public defenders was of interest to the public. There was no reason to doubt that the survey in question contained information which the applicant undertook to impart to the public and which the public had a right to receive. The Court was thus satisfied that access to the requested information was necessary for the applicant to fulfil the task. Lastly, the information was ready and available.

The ECtHR concluded that denial of access to information in that case had impaired the very substance of the freedom to receive information. In reaching this conclusion, it examined in particular the purpose of the information requested and its contribution to an important public debate, the nature of the information sought and whether it had a public interest, and the role played in society by the applicant in the case.

In its reasoning, the Court noted that the study undertaken by the NGO concerned the operation of justice and the right to a fair hearing, which was a right of paramount importance under the ECHR. Since the information requested did not involve data outside the public domain, the privacy rights of the data subjects concerned (the *ex officio* public defenders) would not

109 ECtHR, *Magyar Helsinki Bizottság v. Hungary* [GC], No. 18030/11, 8 November 2016, para. 148.

110 *Ibid.*, paras. 181, 187–200.

have been compromised were the police to give access to the information to the applicant. The information requested by the applicant was of a statistical nature, relating to the number of times the *ex officio* counsel had been appointed to represent defendants in public criminal proceedings.

For the Court, given that the study aimed to contribute to an important debate on a matter of general interest, any restrictions on the NGO proposed publication ought to have been subjected to the utmost scrutiny. The information at stake was of public interest, as public interest covers "matters which are capable of giving rise to considerable controversy, which concern an important social issue, or which involve a problem that the public would have an interest in being informed about".[111] It would thus certainly cover a discussion on the conduct of justice and fair trials, which was the subject matter of the applicant's study. Balancing the different rights at stake and applying the proportionality principle, the ECtHR held that there had been an unjustified violation of the applicant's rights under Article 10 of the ECHR.

1.3.2. Professional secrecy

Under national law, certain communications may be subject to the obligation of professional secrecy. Professional secrecy can be understood as a special ethical duty that incurs a legal obligation inherent in certain professions and functions, which are based on faith and trust. Persons and institutions that fulfil these functions are obliged not to reveal confidential information received by them in the course of performing their duties. Professional secrecy most notably applies to the medical profession and the lawyer-client privilege, with many jurisdictions also acknowledging a professional secrecy obligation on the financial sector. Professional secrecy is not a fundamental right, but is protected as a form of the right to respect for private life. For instance, the CJEU has ruled that in certain cases, "it may be necessary to prohibit the disclosure of certain information which is classified as confidential, in order to protect the fundamental right of an undertaking to respect for its private life enshrined in Article 8 ECHR and Article 7 of the Charter".[112] The ECtHR has also been called to rule on whether restrictions to professional secrecy constitute an infringement of Article 8 of the ECHR, as illustrated in the highlighted examples.

111 *Ibid.*, para. 156.

112 CJEU, Case T-462/12 R, *Pilkington Group Ltd v. European Commission*, Order of the President of the General Court, 11 March 2013, para. 44.

Example: In *Pruteanu v. Romania,*[113] the applicant acted as the lawyer of a commercial company, which had been barred from carrying out bank transactions following allegations of fraud. During the investigation of the case, the Romanian courts authorised the prosecuting authorities to intercept and record a company partner's telephone conversations over a certain period. The recordings and interceptions included his communications with his lawyer.

Mr Pruteanu claimed that this interfered with his right to respect for his private life and correspondence. In its judgment, the ECtHR highlighted the status and importance of a lawyer's relationship with his or her client. The interception of a lawyer's conversations with his client undoubtedly infringed upon professional secrecy, which was the foundation of the relationship between those two people. In such a case, the lawyer could also complain about an interference with his right to respect for private life and correspondence. The CJEU held that there had been a violation of Article 8 of the ECHR.

Example: In *Brito Ferrinho Bexiga Villa-Nova v. Portugal*,[114] the applicant, a lawyer, refused to disclose her personal bank statements to the tax authorities on grounds of professional confidentiality and bank secrecy. The prosecutor's office opened an investigation for tax fraud, and requested authorisation for professional confidentiality to be suspended. The national courts ordered the suspension of confidentiality and bank secrecy rules, finding that the public interest should prevail over the applicant's private interests.

When the case reached the ECtHR, the Court held that accessing the applicant's bank statements constituted an interference with her right to respect for professional confidentiality, which falls within the scope of private life. The interference had a legal basis, as it was based on the code of criminal procedure, and pursued a legitimate aim. However, examining the necessity and proportionality of the interference, the ECtHR pointed to the fact that the proceedings for lifting confidentiality were conducted without the applicant's participation or knowledge. The applicant was thus unable to submit her arguments. In addition, even though domestic law provided

113 ECtHR, *Pruteanu v. Romania*, No. 30181/05, 3 February 2015.

114 ECtHR, *Brito Ferrinho Bexiga Villa-Nova v. Portugal*, No. 69436/10, 1 December 2015.

that the association of lawyers had to be consulted in such proceedings, the association had not been consulted. Finally, the applicant did not have the option to effectively challenge the lifting of confidentiality, nor any remedy by which to challenge the measure. Due to the lack of procedural guarantees and effective judicial control over the measure suspending the duty of confidentiality, the ECtHR concluded that there had been a violation of Article 8 of the ECHR.

The interaction between professional secrecy and data protection is often ambivalent. On the one hand, data protection rules and safeguards established in legislation help ensure professional secrecy. For instance, rules requiring controllers and processors to implement robust data security measures seek to prevent, among other things, loss of confidentiality of personal data protected by professional secrecy. In addition, the EU General Data Protection Regulation enables the processing of health data, which constitute special categories of personal data meriting stronger protection, but makes it subject to the existence of suitable and specific measures to safeguard the rights of data subjects, in particular professional secrecy.[115]

On the other hand, obligations of professional secrecy imposed on controllers and processors in respect of certain personal data may limit rights of the data subjects, notably the right to receive information. Even though the General Data Protection Regulation contains an extensive list with information that, in principle, needs to be provided to the data subject where personal data have not been obtained from him or her, this disclosure requirement does not apply where the personal data must remain confidential due to an obligation of professional secrecy required either by national or EU law.[116]

The General Data Protection Regulation (GDPR) provides for the possibility of Member States adopting, in law, specific rules to safeguard the professional or other equivalent secrecy obligations and reconcile the right to personal data protection with the obligation of professional secrecy.[117]

The GDPR provides that Member States may adopt specific rules on the powers of supervisory authorities in relation to controllers or processors that are subject to an obligation of professional secrecy. These specific rules relate to the power to obtain

115 General Data Protection Regulation, Art. 9 (2) (h) and 9 (3).

116 *Ibid*., Art. 14 (5) (d).

117 *Ibid*., Recital 164 and Art. 90.

access to the premises of a controller or processor, its data-processing equipment and the personal data held, where such personal data have been received in the course of an activity covered by the obligation of secrecy. Thus, the supervisory authorities entrusted with data protection must respect professional secrecy obligations that bind controllers and processors. Moreover, the members of supervisory authorities themselves are also subject to a duty of professional secrecy during and after their term of office. During the exercise of their tasks, members and staff of supervisory authorities may gain knowledge of confidential information. Article 54 (2) of the regulation clearly provides that they have a duty of professional secrecy with regard to such confidential information.

The GDPR requires that Member States notify the Commission of the rules they adopt to reconcile data protection and the principles established in the regulation with the obligation of professional secrecy.

1.3.3. Freedom of religion and belief

Freedom of religion and belief is protected under Article 9 of the ECHR (freedom of thought, conscience and religion) and Article 10 of the EU Charter of Fundamental Rights. Personal data that reveal religious or philosophical beliefs are considered "sensitive data" under both EU and CoE law, and their processing and use is subject to enhanced protection.

Example: The applicant in *Sinak Isik v. Turkey*[118] was a member of the Alevi religious community, whose faith is influenced by Sufism and other pre-Islamic beliefs and is considered by some scholars as a separate religion and by others as part of the Islamic religion. The applicant complained that, against his wishes, his identity card contained a box indicating his religion as "Islam" rather than "Alevi". The domestic courts rejected his request to change his identity card to "Alevi" on the grounds that that word designated a sub-group of Islam and not a separate religion. He then complained before the ECtHR that he had been obliged to disclose his faith, without his consent, because it was mandatory to indicate a person's religion on the identity card and that this was in breach of his right to freedom of religion and conscience, especially given that the designation of "Islam" on his identity card was incorrect.

118 ECtHR, *Sinan Işık v. Turkey*, No. 21924/05, 2 February 2010.

The ECtHR reiterated that religious freedom entails the freedom to manifest a person's religion in community with others, in public and within the circle of persons sharing the same faith, but also alone and in private. The domestic legislation applicable at the time obliged individuals to carry an identity card, a document that had to be shown at the request of any public authority or private enterprises, indicating their religion. Such obligation failed to recognise that the right to manifest one's religion also conferred the reverse, i.e. the right not to be obliged to disclose one's beliefs. Even though the government argued that national legislation had been amended so that individuals could request that the religion box in their identity cards be left blank, in the Court's view the mere fact of having to apply for religion to be deleted could constitute disclosure of information of their attitudes to religion. In addition, when identity cards have a religion box, leaving it empty has a special connotation, as holders of an identity card without information on religion would stand out from those who have a card indicating their beliefs. The ECtHR concluded that domestic legislation was in breach of Article 9 of the ECHR.

The operation of churches and religious associations or communities may, however, require processing members' personal information, to enable communication and the organisation of activities within the congregation. Thus, churches and religious associations have often implemented rules regarding the processing of personal data. According to Article 91 of the General Data Protection Regulation, where such rules are comprehensive they may continue to be valid, provided that they are brought into line with the provisions of the regulation. Churches and religious associations that have such rules must be subject to the oversight of an independent supervisory authority, which might be specific to them, provided that they fulfil the requirements of the General Data Protection Regulation for such authorities.[119]

Religious organisations may undertake the processing of personal data for several reasons – for example, to maintain contact with their congregation or to communicate information about religious or charity events and festivities being organised. In certain states, churches need to keep registers of their members for tax reasons, as membership of religious establishments can have an impact on the taxes payable by individuals. In any case, under European law, data revealing religious beliefs are sensitive data, and churches must be accountable for their handling and processing

119 General Data Protection Regulation, Art. 91 (2).

of such data, especially since information processed by religious organisations often concerns children, the elderly or other vulnerable members of society.

1.3.4. Freedom of the arts and sciences

Another right to balance against the rights to respect for private life and to data protection is the freedom of the arts and sciences, explicitly protected under Article 13 of the EU Charter of Fundamental Rights. This right is deduced primarily from the right to freedom of thought and expression and is to be exercised having regard to Article 1 of the Charter (human dignity). The ECtHR considers that freedom of the arts is protected under Article 10 of the ECHR.[120] The right guaranteed by Article 13 of the Charter may also be subject to the limitations in accordance with Article 52 (1) of the Charter, which may also be interpreted through the lens of Article 10 (2) of the ECHR.[121]

Example: In *Vereinigung bildender Künstler v. Austria,*[122] the Austrian courts prohibited the applicant association from continuing to exhibit a painting that contained photos of the heads of various public figures in sexual positions. An Austrian parliamentarian, whose photo had been used in the painting, brought proceedings against the applicant association, seeking an injunction prohibiting it from exhibiting the painting. The domestic court issued an injunction. The ECtHR reiterated that Article 10 of the ECHR extends to communicating ideas that offend, shock or disturb the state or any section of the population. Those who create, perform, distribute or exhibit works of art contribute to the exchange of ideas and opinions, and the state has the obligation not to encroach unduly on their freedom of expression. Given that the painting was a collage and used photos of only the heads of persons, and that their bodies were painted in an unrealistic and exaggerated manner, which obviously did not aim to reflect or even suggest reality, the ECtHR further stated that "the painting could hardly be understood to address details of [the depicted's] private life, but rather related to his public standing as a politician" and that "in this capacity [the depicted] had to display a wider tolerance in respect of criticism". Weighing the different interests at stake, the ECtHR found that the unlimited prohibition against further exhibiting the painting was disproportionate. The Court concluded that there had been a violation of Article 10 of the ECHR.

120 ECtHR, *Müller and Others v. Switzerland*, No. 10737/84, 24 May 1988.

121 Explanations relating to the Charter of Fundamental Rights, OJ 2007 C 303.

122 ECtHR, *Vereinigung bildender Künstler v. Austria*, No. 68345/01, 25 January 2007, paras. 26 and 34.

European data protection law also acknowledges the special value of science to society. The General Data Protection Regulation and Modernised Convention 108 permit the retention of data for longer periods insofar as the personal data will be processed solely for scientific or historical research purposes. Furthermore, and irrespectively of the original purpose of a specific processing activity, the subsequent use of personal data for scientific research shall not be considered an incompatible purpose.[123] At the same time, appropriate safeguards for such processing must be implemented to protect the rights and freedoms of data subjects. EU or Member State law may provide derogations from the data subject's rights, such as for instance the right to access, rectification, restriction of processing, and to object when it comes to processing their personal data for scientific research, historical or statistical purposes (see also Section 6.1 and Section 9.4).

1.3.5. Protection of intellectual property

A right to the protection of property is enshrined in Article 1 of the First Protocol to the ECHR and also in Article 17 (1) of the EU Charter of Fundamental Rights. One important aspect of the right to property that is particularly relevant for data protection is the protection of intellectual property, explicitly mentioned in Article 17 (2) of the Charter. Several directives in the EU legal order aim to effectively protect intellectual property, in particular copyright. Intellectual property covers not only literary and artistic property but also patent, trademark and associated rights.

As the CJEU's case law has made clear, the protection of the fundamental right to property must be balanced against the protection of other fundamental rights, in particular the right to data protection.[124] There have been cases where copyright protection institutions demanded that internet access providers disclose the identity of users of internet file-sharing platforms. Such platforms often make it possible for internet users to download music titles for free even though these titles are protected by copyright.

> Example: *Promusicae v. Telefónica de España*[125] concerned the refusal of a Spanish internet access provider, Telefónica, to disclose to Promusicae, a non-profit organisation of music producers and publishers of musical and

123 General Data Protection Regulation, Art. 5 (1) (b) and Modernised Convention 108, Art. 5 (4) (b).

124 CJEU, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [GC], 29 January 2008, paras. 62–68.

125 *Ibid*., paras. 54 and 60.

audio-visual recordings, the personal data of certain persons whom it provided with internet access services. Promusicae sought the information's disclosure so that it could initiate civil proceedings against those persons, who it said were using a file exchange program that provided access to phonograms whose exploitation rights were held by Promusicae members.

The Spanish court referred the issue to the CJEU, asking whether such personal data must be communicated, under community law, in the context of civil proceedings to ensure the effective protection of copyright. It referred to Directives 2000/31, 2001/29 and 2004/48, read also in light of Articles 17 and 47 of the Charter. The CJEU concluded that these three directives, as well as the e-Privacy Directive (Directive 2002/58), do not preclude Member States from laying down an obligation to disclose personal data in the context of civil proceedings to ensure effective copyright protection.

The CJEU pointed out that the case therefore raised the question of the need to reconcile the requirements of the protection of different fundamental rights – namely, the right to respect for private life with the rights to protection of property and to an effective remedy.

It concluded that "the Member States must, when transposing the directives mentioned above, take care to rely on an interpretation of those directives which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality".[126]

Example: *Bonnier Audio AB and Others v. Perfect Communication Sweden AB*[127] concerned the balance between intellectual property rights and personal data protection. The applicants – five publishing companies holding copyrights on 27 audiobooks – brought proceedings before the Swedish court, alleging that

126 *Ibid.*, paras. 65 and 68; see also CJEU, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, 16 February 2012.

127 CJEU, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v. Perfect Communication Sweden AB*, 19 April 2012.

these copyrights were infringed by means of a FTP server (a file transfer protocol that allows file sharing and data transfer via the internet). The applicants requested the internet service provider (ISP) to disclose the name and address of the person using the IP address from which the files were sent. The ISP, ePhone, challenged the application, alleging that it violated the Directive 2006/24 (the Data Retention Directive – invalidated in 2014).

The Swedish court referred the issue to the CJEU, asking whether Directive 2006/24 precludes the application of a national provision based on Article 8 of Directive 2004/48 (Intellectual Property Rights Enforcement Directive), which allows issuing an injunction requiring ISPs to transmit to copyright holders information on subscribers whose IP addresses were allegedly used in infringements. The question was based on the assumption that the applicant has adduced clear evidence of the infringement of a particular copyright and that the measure is proportionate.

The CJEU pointed out that Directive 2006/24 dealt exclusively with the handling and retention of data generated by electronic communication service providers for the purpose of the investigation, detection, and prosecution of serious crime and their communication to competent national authorities. Thus, a national provision transposing the Intellectual Property Rights Enforcement Directive is outside the scope of Directive 2006/24 and therefore not precluded by that directive.[128]

As regards the communication of the name and address in question, sought by the applicants, the CJEU held that such action constitutes processing of personal data, and falls within the scope of Directive 2002/58 (e-Privacy Directive). It also noted that the communication of those data was required in civil proceedings for the benefit of a copyright holder to ensure effective protection of copyright and thus also falls, by its very object, within the scope of Directive 2004/48.[129]

The CJEU concluded that Directives 2002/58 and 2004/48 must be interpreted as not precluding national legislation such as that at issue in the main proceedings, insofar as that legislation enables the national court seized

128 *Ibid.*, para. 40–41.

129 *Ibid.*, paras. 52–54. See also CJEU, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [GC], 29 January 2008, para. 58.

by an application for an order for disclosure of personal data to weigh the conflicting interests involved, on the basis of the facts of each case and taking due account of the requirements of the principle of proportionality.

1.3.6. Data protection and economic interests

In the digital age or age of big data, data have been described as "the new oil" of the economy for boosting innovation and creativity.[130] Many companies have built robust business models around data processing, and such processing often involves personal data. Certain companies may believe that specific rules related to personal data protection may, in practice, result in overly burdensome obligations that could affect their economic interests. Thus, a question arises as to whether the economic interests of controllers and processors, or of the general public, could justify limiting the right to data protection.

Example: In *Google Spain*,[131] the CJEU held that, under certain conditions, individuals have the right to request search engines to remove search results from their search index. In its reasoning, the CJEU pointed to the fact that the use of search engines and the listed search results can establish a detailed profile of an individual. This information may concern a vast aspect of an individual's private life and could not have been easily found or interconnected without a search engine. It thus constituted a potentially serious interference with the data subjects' fundamental rights to privacy and protection of personal data.

The CJEU then examined whether the interference could be justified. With regard to the search engine company's economic interest in conducting the processing, the CJEU stated that "it is clear that [the interference] cannot be justified by merely the economic interest which the operator of such an engine has in that processing", and that "as a rule" the fundamental rights under Articles 7 and 8 of the Charter override such economic interest and the interest of the general public in finding that information upon a search relating to the data subject's name.[132]

130 See, for example, *Financial Times* (2016), "Data is the new oil... who's going to own it?", 16 November 2016.

131 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 May 2014.

132 *Ibid.*, paras. 81 and 97.

One of the key considerations of European data protection law is to provide individuals with more control over their personal data. Especially in the digital age, there is an imbalance between the power of business entities that process and have access to vast amounts of personal data and the power of the individuals to whom those personal data belong to control their information. The CJEU takes a case-by-case approach when balancing data protection and economic interests – such as the interests of third parties in relation to joint stock and limited liability companies, as illustrated in the *Manni* judgment.

Example: The *Manni* case[133] concerned the inclusion of an individual's personal data in a public commercial register. Mr Manni had requested the Lecce Chamber of Commerce to delete his personal data from that registry, having discovered that potential clients would resort to the registry and see that he had been the administrator of a company which was declared bankrupt more than a decade before. This information prejudiced his potential clients and could have a negative impact on his commercial interests.

The CJEU was called upon to determine if EU law recognised a right to erasure in that case. In reaching its conclusion, it balanced EU data protection rules and Mr Manni's commercial interest in removing the information about his former company's bankruptcy, with the public interest in access to the information. It took due note of the fact that disclosure to the public registry of companies was provided for by law, and particularly by an EU Directive aiming to make company information more easily accessible to third parties. The disclosure was important to protect the interests of third parties who may want to conduct business with a specific company, because the only safeguards offered by joint-stock companies and limited liability companies to third parties are their assets. Therefore, "the basic documents of the company concerned should be disclosed in order that third parties may be able to ascertain their contents and other information concerning the company, especially particulars of the persons who are authorised to bind the company".[134]

In view of the importance of the legitimate aim pursued by the register, the CJEU held that Mr Manni did not have a right to obtain erasure of his

133 CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 9 March 2017.

134 *Ibid*., para. 49.

personal data, as the need to protect the interests of third parties in relation to joint-stock and limited liability companies, and to ensure legal certainty, fair trading and thus the proper functioning of the internal market, took precedence over his rights under data protection legislation. This was particularly so in view of the fact that individuals choosing to participate in trade through a joint stock or limited liability company are aware that they are required to disclose information relating to their identity and functions.

While finding that there were no grounds to obtain erasure in this case, the CJEU did acknowledge the existence of a right to object to the processing, noting: "it cannot be excluded [...] that there may be specific situations in which the overriding and legitimate reasons relating to the specific case of the person concerned justify exceptionally that access to personal data entered in the register is limited, upon the expiry of a sufficiently long period [...] to third parties who can demonstrate a specific interest in their consultation".[135]

The CJEU stated that it is up to the national courts to assess in each case, and having regard to all the relevant circumstances of the individual, the existence or absence of legitimate and overriding reasons which could exceptionally justify the restriction of third parties' access to personal data contained in company registers. However, it clarified that, in the case of Mr Manni, the mere fact that disclosure of his personal data in the register allegedly affected his clientele could not be considered such a legitimate and overriding reason. Potential clients of Mr Manni have a legitimate interest in information regarding the bankruptcy of his previous company.

The interference with the fundamental rights of Mr Manni and other persons included in the registry to respect for private life and to protection of personal data as guaranteed by Articles 7 and 8 of the Charter served an objective of general interest and was necessary and proportionate.

In *Manni*, therefore, the CJEU held that the rights to data protection and privacy did not prevail over the interest of third parties to access the information in the companies' register in relation to joint-stock companies and limited liability companies.

135 *Ibid.*, para. 60.

2 Data protection terminology

EU	Issues covered	CoE
Personal data		
General Data Protection Regulation, Article 4 (1) General Data Protection Regulation, Articles 4 (5) and 5 (1) (e) General Data Protection Regulation, Article 9 CJEU, Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 2010 CJEU, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [GC], 2008 CJEU, C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 CJEU, C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, 2016 CJEU, Joined cases C-141/12 and C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel* and *Minister voor Immigratie, Integratie en Asiel v. M and S*, 2014	**Legal definition of data protection**	Modernised Convention 108, Article 2 (a) ECtHR, *Bernh Larsen Holding AS and Others v. Norway*, No. 24117/08, 2013 ECtHR, *Uzun v. Germany*, No. 35623/05, 2010 ECtHR, *Amann v. Switzerland* [GC], No. 27798/95, 2000
CJEU, C-101/01, *Criminal proceedings against Bodil Lindqvist*, 2003	**Special categories of personal data (sensitive data)**	Modernised Convention 108, Article 6 (1)
CJEU, C-434/16, *Peter Nowak v. Data Protection Commissioner*, 2017	**Anonymised and Pseudonymised personal data**	Modernised Convention 108, Article 5 (4) (e) Explanatory Report of Modernised Convention 108, Paragraph 50

EU	Issues covered	CoE
Data processing		
General Data Protection Regulation, Article 4 (2) CJEU, C-212/13, *František Ryneš v.* Úřad *pro ochranu osobních* údajů, 2014 CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 2017 CJEU, C-101/01, *Criminal proceedings against Bodil Lindqvist*, 2003 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014	**Definitions**	Modernised Convention 108, Article 2 (b) and (c)
Data users		
General Data Protection Regulation, Article 4 (7) CJEU, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, 2014 CJEU, C-1318/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014	**Controller**	Modernised Convention 108, Article 2 (d) Profiling Recommendation, Article 1 (g)*
General Data Protection Regulation, Article 4 (8)	**Processor**	Modernised Convention 108, Article 2 (f) Profiling Recommendation, Article 1 (h)
General Data Protection Regulation, Article 4 (9)	**Recipient**	Modernised Convention 108, Article 2 (e)
General Data Protection Regulation, Article 4 (10)	**Third party**	
Consent		
General Data Protection Regulation, Articles 4 (11) and 7 CJEU, C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, 2011 CJEU, C-536/15, *Tele2 (Netherlands) BV and Others v. Autoriteit Consument en Markt (AMC)*, 2017	**Definition and requirements for valid consent**	Modernised Convention 108, Article 5 (2) Medical Data Recommendation, Article 6, and various subsequent recommendations ECtHR, *Elberte v. Latvia*, No.61243/08, 2015

*Note: * Council of Europe, Committee of Ministers (2010), Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Profiling Recommendation), 23 November 2010.*

2.1. Personal data

Key points

- Data are personal data if they relate to an identified or identifiable person, the 'data subject'.
- To determine whether a natural person is identifiable, either a controller or another person should take into account all reasonable means that are likely to be used – such as singling out – to directly or indirectly identify the natural person.
- Authentication means proving that a certain person possesses a certain identity and/or is authorised to carry out certain activities.
- There are special categories of data, so-called sensitive data, listed in Modernised Convention 108 and in EU Data Protection law, which require enhanced protection and, therefore, are subject to a special legal regime.
- Data are anonymised if they no longer relate to an identified or identifiable individual.
- Pseudonymisation is a measure by which personal data cannot be attributed to the data subject without additional information, which is kept separately. The 'key' that enables re-identification of the data subjects must be kept separate and secure. Data that have undergone a pseudonymisation process remain personal data. There is no concept of 'pseudonymised data' under EU law.
- The principles and rules of data protection do not apply to anonymised information. However, they do apply to pseudonymised data.

2.1.1. Main aspects of the concept of personal data

Under EU law as well as **under CoE law**, 'personal data' is defined as information relating to an identified or identifiable natural person.[136] It concerns information about a person whose identity is either manifestly clear or can be established from additional information. To determine whether a person is identifiable, a controller or another person must take into account all reasonable means that are likely to be used to directly or indirectly identify the individual, such as, for example, singling out, which makes it possible to treat one person differently from another.[137]

If data about such a person are being processed, this person is called the 'data subject'.

136 General Data Protection Regulation, Art. 4 (1); Modernised Convention 108, Art. 2 (a).

137 General Data Protection Regulation, Recital 26.

The data subject

Under EU law, natural persons are the only beneficiaries of data protection rules[138] and only living beings are protected under European data protection law.[139] The General Data Protection Regulation (GDPR) defines personal data as any information relating to an identified or identifiable natural person.

CoE law, notably Modernised Convention 108, also refer to the protection of individuals regarding the processing of their personal data. There too, personal data means any information relating to an identified or identifiable individual. This natural person or individual, as referred to in the GDPR and Modernised Convention 108 respectively, is known in data protection law as the data subject.

Legal persons also have some protection. ECtHR case law exists giving judgment on applications of legal persons alleging violations of their right to protection against the use of their data under Article 8 of the ECHR. Article 8 of the ECHR covers both the right to respect for private and family life, and for home and correspondence. The Court can therefore examine cases under the latter, rather than under private life.

Example: *Bernh Larsen Holding AS and Others v. Norway*[140] concerned a complaint by three Norwegian companies about a tax authority decision ordering them to provide the tax auditors with a copy of all the data held on a computer server they used jointly.

The ECtHR found that such an obligation on the applicant companies constituted an interference with their rights to respect for 'home' and 'correspondence' under Article 8 of the ECHR. The Court found, however, that the tax authorities had effective and adequate safeguards against abuse: the applicant companies had been notified well in advance; were present and able to make submissions during the on-site intervention; and the material was to be destroyed once the tax review was completed. In such circumstances, a fair balance had been struck between the applicant companies' right to respect for 'home' and 'correspondence' and their interest

138 *Ibid.*, Art. 1.

139 *Ibid.*, Recital 27. See also Article 29 Working Party (2007), *Opinion 4/2007 on the concept of personal data*, WP 136, 20 June 2007, p. 22.

140 ECtHR, *Bernh Larsen Holding AS and Others v. Norway*, No. 24117/08, 14 March 2013. See also, however, ECtHR, *Liberty and Others v. the United Kingdom*, No. 58243/00, 1 July 2008.

in protecting the privacy of persons working for them, on the one hand, and the public interest in ensuring efficient inspection for tax assessment purposes, on the other. The Court held that there had, therefore, been no violation of Article 8.

According to Modernised Convention 108, data protection deals, primarily, with the protection of natural persons; however, the Contracting Parties may extend data protection to legal persons such as businesses and associations in their domestic law. The Explanatory Report to the Modernised Convention states that national law may protect the legitimate interests of legal persons by extending the scope of the convention to such actors.[141] **EU data protection law** does not cover data processing which concern legal persons, and in particular does not concern undertakings established as legal persons, including the name and form of the legal person and their contact details.[142] The e-Privacy Directive does, however, protect the confidentiality of communications and the legitimate interests of legal persons concerning the increasing capacity for the automated storage and processing of data relating to subscribers and users.[143] Similarly, the draft e-Privacy Regulation extends protection to legal persons.

Example: In *Volker und Markus Schecke and Hartmut Eifert v. Land Hessen*,[144] the CJEU, referring to the publication of personal data relating to beneficiaries of agricultural aid, held that "legal persons can claim the protection of Articles 7 and 8 of the Charter in relation to such identification only in so far as the official title of the legal person identifies one or more natural persons. […T]he right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter, concerns any information relating to an identified or identifiable individual […]".[145]

Balancing the interest of the EU to ensure transparency in allocating aid on the one hand, and the fundamental rights to privacy and data protection of the individuals who benefited from the aid on the other hand, the CJEU considered that the interference with those fundamental rights was

141 Explanatory Report of Modernised Convention 108, para. 30.

142 General Data Protection Regulation, Recital 14.

143 e-Privacy Directive, Recital 7 and Art. 1 (2).

144 CJEU, Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 9 November 2010, para. 53.

145 *Ibid*., paras. 52–53.

disproportionate. It considered that the transparency objective could have been effectively achieved by measures that are less intrusive to the rights of the individuals concerned. However, when examining the proportionality of publishing information concerning legal persons who received aid, the CJEU reached a different conclusion, ruling that such publication did not go beyond the limits of the proportionality principle. It stated that "the seriousness of the breach of the right to protection of personal data manifests itself in different ways for, on the one hand, legal persons and, on the other hand, natural persons".[146] Legal persons were subject to more onerous obligations concerning the publication of information relating to them. The CJEU considered that requiring national authorities to examine whether the data of each beneficiary legal person identifies any associated natural persons before publishing the data, would impose an unreasonable administrative burden on those authorities. Therefore, the legislation requiring a generalised publication of data relating to legal persons had struck a fair balance between the competing interests at stake.

Nature of the data

Any kind of information can be personal data provided that it relates to an identified or identifiable person.

Example: A supervisor's assessment of an employee's work performance, stored in the employee's personnel file, is personal data about the employee. This is the case even though it may just reflect, in part or whole, the superior's personal opinion, such as: "the employee is not dedicated to their work" – and not hard facts, such as: "the employee has been absent from work for five weeks during the last six months".

Personal data covers information pertaining to the private life of a person, which also includes professional activities, as well as information about his or her public life.

In the *Amann* case,[147] the ECtHR interpreted the term 'personal data' as not being limited to matters of the private sphere of an individual. This meaning of the term 'personal data' is also relevant for the GDPR.

146 *Ibid.*, para. 87.

147 See ECtHR, *Amann v. Switzerland,* No. 27798/95, 16 February 2000, para. 65.

Example: In *Volker und Markus Schecke and Hartmut Eifert v. Land Hessen*,[148] the CJEU stated that "it is of no relevance in this respect that the data published concerns activities of a professional nature [...]. The European Court of Human Rights has held on this point, with reference to the interpretation of Article 8 of Convention 108, that the term 'private life' must not be interpreted restrictively and that there is no reason of principle to justify excluding activities of a professional [...] nature from the notion of private life".

Example: In the joined cases *YS v. Minister voor Immigratie, Integratie en Asiel* and *Minister voor Immigratie, Integratie en Asiel v. M and S*,[149] the CJEU stated that the legal analysis contained in a draft decision of the Immigration and Naturalisation Service dealing with residence permit applications does not in itself constitute personal data, even though it may include some personal data.

The ECtHR's case law concerning Article 8 of the ECHR confirms that it may be difficult to completely separate matters of private and professional life.[150]

Example: In *Bărbulescu v. Romania*,[151] the applicant had been dismissed for using his employer's internet during working hours in breach of internal regulations. His employer had monitored his communications and the records, which showed messages of a purely private nature, were produced during the domestic proceedings. In finding Article 8 to be applicable, the ECtHR left open the question of whether the employer's restrictive regulations left the applicant with a reasonable expectation of privacy, but in any event found that an employer's instructions could not reduce private social life in the workplace to zero. As regards the merits, Contracting States had to be granted a wide margin of appreciation in assessing the need to establish a legal framework governing the conditions in which an employer could regulate its employees' non-professional communications – electronic or

148 CJEU, Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 9 November 2010, para. 59.

149 CJEU, Joined cases C-141/12 and C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel* and *Minister voor Immigratie, Integratie en Asiel v. M and S*, 17 July 2014, para. 39.

150 See, for example, ECtHR, *Rotaru v. Romania* [GC], No. 28341/95, 4 May 2000, para. 43; ECtHR, *Niemietz v. Germany*, No. 13710/88, 16 December 1992, para. 29.

151 ECtHR, *Bărbulescu v. Romania* [GC], No. 61496/08, 5 September 2017, para. 121.

other forms – in the workplace. Nevertheless, the domestic authorities had to ensure that an employer's introduction of measures to monitor correspondence and other communications, irrespective of the extent and duration of such measures, was accompanied by adequate and sufficient safeguards against abuse. Proportionality and procedural guarantees against arbitrariness were essential and the ECtHR identified a number of factors which were relevant in the circumstances. Such factors included, for example, the extent of the employer's monitoring of employees and the degree of intrusion into the employee's privacy, the consequences for the employee and whether adequate safeguards had been provided. In addition, domestic authorities had to ensure that an employee whose communications had been monitored had access to a remedy before a judicial body with jurisdiction to determine, at least in substance, how those criteria outlined were observed and whether the impugned measures were lawful. In this case, the ECtHR found a violation of Article 8 because the domestic authorities had not afforded adequate protection of the applicant's right to respect for his private life and correspondence and had consequently failed to strike a fair balance between the interests at stake.

Under EU law as well as **under CoE law**, information contains data about a person if:

- an individual is identified or identifiable by this information; or
- an individual, while not identified, can be singled out by this information in a way which makes it possible to find out who the data subject is by conducting further research.

Both types of information are protected in the same manner under European data protection law. Direct or indirect identifiability of individuals requires continuous assessment, "taking into consideration the available technology at the time of the processing and technology developments".[152] The ECtHR has repeatedly stated that the notion of 'personal data' under the ECHR is the same as in Convention 108, especially concerning the condition of relating to identified or identifiable persons.[153]

The GDPR stipulates that a natural person is identifiable when he or she "can be identified, directly or indirectly, in particular by reference to an identifier such as a

152 General Data Protection Regulation, Recital 26.

153 See ECtHR, *Amann v. Switzerland* [GC], No. 27798/95, 16 February 2000, para. 65.

name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person".[154] Identification thus requires elements which describe a person in such a way that he or she is distinguishable from all other persons and recognisable as an individual. A person's name is a prime example of such elements of description, and can directly identify a person. In some cases, other attributes can have a similar effect to a name, making a person indirectly identifiable. A telephone number, social security number and vehicle registration number are all examples of information that can make an individual identifiable. It is also possible to use attributes – such as computerised files, cookies and web traffic surveillance tools – to single out individuals by identifying their behaviour and habits. As explained in an opinion of the Article 29 Working Party, "[w]ithout even enquiring about the name and address of the individual it is possible to categorise this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer requires the disclosure of his or her identity in the narrow sense".[155] The definition of personal data under both the CoE and the EU is broad enough to cover all possibilities of identification (and, therefore, all degrees of identifiability).

Example: In *Promusicae v. Telefónica de España*,[156] the CJEU stated that "it is not disputed that the communication sought by Promusicae of the names and addresses of certain users of [a certain internet file-sharing platform] involves the making available of personal data, that is, information relating to identified or identifiable natural persons, in accordance with the definition in Article 2 (a) of Directive 95/46 [currently Article 4 (1) of the GDPR]. That communication of information which, as Promusicae submits and Telefónica does not contest, is stored by Telefónica constitutes the processing of personal data".[157]

Example: *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*[158] concerned the refusal of the internet service

154 General Data Protection Regulation, Art. 4 (1).

155 Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, WP 136, 20 June 2007, p. 15.

156 CJEU, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [GC], 29 January 2008, para. 45.

157 Former Directive 95/46, Art. 2 (b), now General Data Protection Regulation, Art. 4 (2).

158 CJEU, C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 November 2011, para. 51.

provider Scarlet to install a system to filter electronic communications that use file-sharing software to prevent file-sharing that infringes copyright protected by SABAM, a management company that represents authors, composers and editors. The CJEU held that users' IP addresses "are protected personal data because they allow those users to be precisely identified".

As many names are not unique, establishing the identity of a person may need additional attributes to ensure that a person is not mistaken for someone else. Sometimes, direct and indirect attributes may have to be combined to identify the individual to whom the information relates. Date and place of birth are often used. In addition, personalised numbers have been introduced in some countries to better distinguish between citizens. Transferred tax data,[159] data pertaining to an applicant for a residence permit contained in an administrative document,[160] and documents concerning banking and fiduciary relationships[161] may be personal data. Biometric data, such as fingerprints, digital photos or iris scans, location data and online attributes are increasingly used to identify persons in the technological age.

For the applicability of European data protection law, however, there is no need for actual identification of the data subject; it is sufficient that the person concerned be identifiable. A person is considered identifiable if there are enough elements available through which the person can be directly or indirectly identified.[162] According to Recital 26 of the GDPR, the benchmark is whether it is likely that reasonable means for identification will be available and administered by the foreseeable users of the information; this includes information held by third-party recipients (see Section 2.3.2).

Example: A local authority decides to collect data about cars speeding on local streets. It photographs the cars, automatically recording the time and location, in order to pass the data on to the competent authority so that it can fine those who violated the speed limits. A data subject files a complaint, claiming that the local authority has no legal basis under data protection law for such data collection. The local authority maintains that it does not collect

159 CJEU, C-201/14, *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others*, 1 October 2015.

160 CJEU, *YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S*, 17 July 2014.

161 ECtHR, *M.N. and Others v. San Marino*, No. 28005/12, 7 July 2015.

162 General Data Protection Regulation, Art. 4 (1).

personal data. Licence plates, it says, are anonymous. The local authority has no legal authority to access the general vehicle register to find out the identity of the car owner or driver.

This reasoning is not in accordance with Recital 26 of the GDPR. Given that the purpose of the data collection is clearly to identify and fine speeders, it is foreseeable that identification will be attempted. Although the local authorities do not have a means of identification directly available to them, they will pass on the data to the competent authority, the police, who does have such means. Recital 26 also explicitly includes a scenario where it is foreseeable that further data recipients, other than the immediate data user, may attempt to identify the individual. In light of Recital 26, the local authority's action equates to collecting data about identifiable persons and, therefore, requires a legal basis under data protection law.

To "ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the cost of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments".[163]

Example: In *Breyer v. Bundesrepublik Deutschland*,[164] the CJEU considered the notion of indirect identifiability of data subjects. The case dealt with dynamic IP addresses, which change every time a new connection is made to the internet. The websites run by federal German institutions registered and stored dynamic IP addresses to prevent cyber-attacks and to initiate criminal proceedings where needed. Only the internet service provider that Mr Breyer used had the additional information needed to identify him.

The CJEU considered that a dynamic IP address, which an online media services provider registers when a person accesses a website that the provider has made accessible to the public, constitutes personal data where only a third party – the internet service provider in this case – has the additional data necessary to identify the person.[165] It held that "it is not

163 *Ibid*., Recital 26.

164 CJEU, C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, 19 October 2016, para. 43.

165 Former Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Art. 2 (a).

required that all information enabling the identification of the data subject must be held in the hands of one person" for information to constitute personal data. Users of a dynamic IP address registered by an internet service provider may be identified in certain situations, for instance within the framework of criminal proceedings in the event of cyber-attacks, with the assistance of other persons.[166] According to the CJEU, when the provider "has the legal means which enable it to identify the data subject with additional data which the internet provider has about that person", this constitutes "a means likely reasonable to be used to identify the data subject". Therefore, such data are considered personal data.

Under CoE law, identifiability is understood in a similar way. The Explanatory Report of Modernised Convention 108 includes a similar description: the notion of 'identifiable' does not only refer to the individual's civil or legal identity as such, but also to what may allow one person to be 'individualised' or singled out from others, and as a result, potentially treated differently. This 'individualisation' could be done, for instance, by referring to him or her specifically, or to a device or a combination of devices (computer, mobile phone, camera, gaming devices, etc.) linked to an identification number, a pseudonym, biometric or genetic data, location data, an IP address, or another identifier.[167] An individual is not considered 'identifiable' if his or her identification requires unreasonable time, effort or resources. Such is the case, for example, when identifying a data subject would require excessively complex, long and costly operations. The unreasonableness of time, effort or resources must be assessed on a case-by-case basis which takes into consideration factors such as the processing purpose of the processing, the cost and benefits of identification, the type of controller and the technology used.[168]

As to the form in which the personal data is stored or used, it is important to note that it is not relevant to the applicability of data protection law. Written or spoken communications may contain personal data as well as images,[169] including closed-

166 CJEU, C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 November 2011, paras. 47–48.

167 Explanatory Report of Modernised Convention 108, para. 18.

168 *Ibid.*, para. 17.

169 ECtHR, *Von Hannover v. Germany*, No. 59320/00, 24 June 2004; ECtHR, *Sciacca v. Italy*, No. 50774/99, 11 January 2005; CJEU, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, 11 December 2014.

circuit television (CCTV) footage[170] or sound.[171] Electronically recorded information and information on paper may also be personal data. Even cell samples of human tissue – which record a person's DNA – may be sources from which biometric data can be extracted,[172] as long as the data relate to the individual's inherited or acquired genetic characteristics, provide unique information about their health or physiology, and result from an analysis of a biological sample from that person.[173]

Anonymisation

According to the principle of storage limitation contained in both the GDPR and Modernised Convention 108 (discussed in more detail in Chapter 3), data must be kept "in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed".[174] Consequently, data would have to be erased or anonymised if a controller wanted to store them after they were no longer needed and no longer served their initial purpose.

The process of anonymising data means that all identifying elements are eliminated from a set of personal data so that the data subject is no longer identifiable.[175] In its Opinion 05/2014, the Article 29 Working Party analyses the effectiveness and limits of different anonymisation techniques.[176] It acknowledges the potential value of such techniques, but underlines that certain techniques do not necessarily work in all cases. To find the optimal solution in a given situation, the appropriate process of anonymisation should be decided on a case-by-case basis. Irrespective of the technique used, identification must be prevented, irreversibly. This means that for data to be anonymised, no element may be left in the information which could, by exercising reasonable effort, serve to re-identify the person(s) concerned.[177] The risk of re-identification can be assessed by taking into account "the time, effort or

170 ECtHR, *Peck v. the United Kingdom*, No. 44647/98, 28 January 2003; ECtHR, *Köpke v. Germany* (dec.), No. 420/07, 5 October 2010; EDPS (2010), *The EDPS video-surveillance guidelines*, 17 March 2010.

171 ECtHR, *P.G. and J.H. v. the United Kingdom*, No. 44787/98, 25 September 2001, paras. 59–60; ECtHR, *Wisse v. France*, No. 71611/01, 20 December 2005 (French language version).

172 See Article 29 Working Party (2007), *Opinion 4/2007 on the concept of personal data*, WP136, 20 June 2007, p. 9; Council of Europe, Recommendation No. Rec (2006) 4 of the Committee of Ministers to member states on research on biological materials of human origin, 15 March 2006.

173 General Data Protection Regulation, Art. 4 (13).

174 *Ibid.*, Art. 5 (1) (e); Modernised Convention 108, Art. 5 (4) (e).

175 General Data Protection Regulation, Recital 26.

176 Article 29 Working Party (2014), *Opinion 05/2014 on Anonymization Techniques*, WP216, 10 April 2014.

177 General Data Protection Regulation, Recital 26.

resources needed in light of the nature of the data, the context of their use, the available re-identification technologies and related costs".[178]

When data have been successfully anonymised, they are no longer personal data and data protection legislation no longer applies.

The GDPR provides that the person or organisation controlling the personal data processing cannot be obliged to maintain, acquire or process additional information to identify the data subject for the sole purpose of complying with the regulation. However, this rule has a significant exemption: whenever the data subject, for the purpose of exercising the rights of access, rectification, erasure, restriction of the processing and data portability, provides additional information to the controller enabling his or her identification, then those data which were previously anonymised become personal data again.[179]

Pseudonymisation

Personal information contains attributes, such as name, date of birth, sex, address, or other elements that could lead to identification. The process of pseudonymising personal data means that these attributes are replaced by a pseudonym.

EU law defines 'pseudonymisation' as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".[180] Contrary to anonymised data, pseudonymised data are still personal data and are therefore subject to data protection legislation. Although pseudonymisation can reduce security risks to the data subjects, it is not exempt from the scope of the GDPR.

The GDPR recognises various uses of pseudonymisation as an appropriate technical measure for enhancing data protection, and is specifically mentioned for the design and security of its data processing.[181] It is also an appropriate safeguard that could be

178 Council of Europe, Committee of Convention 108 (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23 January 2017, para. 6.2.

179 General Data Protection Regulation, Art. 11.

180 *Ibid.*, Art. 4 (5).

181 *Ibid.*, Art. 25 (1).

used to process personal data for purposes other than for which they were initially collected.[182]

Pseudonymisation is not explicitly mentioned in the legal definition of the **CoE** Modernised Convention 108. However, the Explanatory Report of Modernised Convention 108 clearly states that "the use of a pseudonym or of any digital identifier/digital identity does not lead to anonymisation of the data as the data subject can still be identifiable or individualised".[183] One way to pseudonymise data is through data encryption. Once data has been pseudonymised, the link to an identity exists in the form of the pseudonym plus a decryption key. Without such a key, it is difficult to identify pseudonymised data. However, for those entitled to use the decryption key, re-identification is easily possible. The use of encryption keys by unauthorised persons must be particularly guarded against. Therefore, "[p]seudonymous data is [...] to be considered a personal data [...]" covered by Modernised Convention 108.[184]

Authentication

This is a procedure by which a person is able to prove that he or she possesses a certain identity and/or is authorised to do certain things, such as enter a security area, or withdraw money from a banking account. Authentication can be achieved by comparing biometric data, such as a photo or fingerprints in a passport, with the data of the person presenting himself or herself, for example, at immigration control;[185] or by asking for information which should be known only to the person with a certain identity or authorisation, such as a personal identification number (PIN) or password; or by requiring the presentation of a certain token, which should be exclusively in the possession of the person with a certain identity or authorisation, such as a special chip card or key to a banking safe. Apart from passwords or chip cards, electronic signatures – sometimes together with PINs – are an instrument especially capable of identifying and authenticating a person in electronic communications.

182 *Ibid*., Art. 6 (4).

183 Explanatory Report of Modernised Convention 108, para. 18.

184 *Ibid*.

185 *Ibid*., paras.56–57.

2.1.2. Special categories of personal data

Under EU law as well as **CoE law**, there are special categories of personal data which, by their nature, may pose a risk to the data subjects when processed and need enhanced protection. Such data are subject to a prohibition principle and there are a limited number of conditions under which such processing is lawful.

Within the framework of Modernised Convention 108 (Article 6) and the GDPR (Article 9), the following categories are considered sensitive data:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions, religious or other beliefs, including philosophical beliefs;
- personal data revealing trade union membership;
- genetic data and biometric data processed for the purpose of identifying a person;
- personal data concerning health, sexual life or sexual orientation.

Example: *Bodil Lindqvist*[186] concerned the reference to different persons by name or by other means, such as their telephone number or information on their hobbies, on an internet page. The CJEU stated that "reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health".[187]

Personal data relating to criminal convictions and offences

Modernised Convention 108 includes personal data relating to offences, criminal proceedings and convictions, and related security measures in the list of special categories of personal data.[188] Within the framework of the GDPR, personal data relating to criminal convictions and offences or related security measures are not mentioned as such in the list of special categories of data, but are dealt with in a separate

186 CJEU, C-101/01, *Criminal proceedings against Bodil Lindqvist*, 6 November 2003, para. 51.

187 Former Directive 95/46/EC, Art. 8 (1), now General Data Protection Regulation Art. 9 (1).

188 Modernised Convention 108, Art. 6 (1).

article. Article 10 of the GDPR stipulates that processing such data may only be carried out "under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects". Comprehensive registers holding information on criminal convictions, on the other hand, can only be kept under the control of specific official authorities.[189] In the EU, processing personal data in the context of law enforcement is governed by a specific legal instrument, Directive 2016/680/EU.[190] The directive stipulates specific rules for data protection, which are binding upon competent authorities when they process personal data specifically to prevent, investigate, detect and prosecute criminal offences (see Section 8.2.1).

2.2. Data processing

Key points

- 'Data processing' concerns any operation performed on personal data.
- The term 'processing' covers automated and non-automated processing.
- Under EU law, 'processing' also refers to manual processing in structured filing systems.
- Under CoE law, the meaning of 'processing' can be extended by domestic law to include manual processing.

2.2.1. The concept of data processing

The concept of personal data processing is comprehensive **under both EU and CoE law:** "'processing of personal data' [...] shall mean any operation [...] such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"[191] of

189 General Data Protection Regulation, Art. 10.

190 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119.

191 General Data Protection Regulation, Art. 4 (2). See also Modernised Convention 108, Art. 2 (b).

personal data. Modernised Convention 108 adds the preservation of personal data to the definition.[192]

Example: In *František Ryneš*,[193] Mr Ryneš captured the image of two individuals who broke windows in his home through the domestic CCTV surveillance system he had installed to protect his property. The CJEU determined that video surveillance involving the recording and storage of personal data constitutes automatic data processing that falls within the scope of EU data protection law.

Example: In *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*,[194] Mr Manni requested the removal of his personal data from a rating company's register that linked him to the liquidation of a real estate company, thereby having a negative impact on his reputation. The CJEU held that "by transcribing and keeping that information in the register and communicating it, where appropriate, on request to third parties, the authority responsible for maintaining that register carries out 'processing of personal data' for which it is the 'controller'".

Example: Employers collect and process data about their employees, including information relating to their salaries. Their employment agreements provide the legal ground for legitimately doing so.

Employers will have to forward their staff's salary data to the tax authorities. This transmission of data will also be 'processing' under the meaning of this term in Modernised Convention 108 and in the GDPR. The legal ground for such disclosure, however, is not the employment agreements. There must be an additional legal basis for the processing operations which result in employer's transmitting salary data to the tax authorities. This legal basis is usually to be found in the provisions of national tax laws. Without such provisions – and in the absence of any other legitimate ground for processing – this transmission of personal data would be unlawful processing.

192 Modernised Convention 108, Art. 2 (b).

193 CJEU, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, 11 December 2014, para. 25.

194 CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 9 March 2017, para. 35.

2.2.2. Automated data processing

Data protection under Modernised Convention 108 and the GDPR fully applies to automated data processing.

Under **EU law**, automated data processing concerns operations performed on "personal data wholly or partly by automated means".[195] Modernised Convention 108 includes a similar definition.[196] In practical terms, this means that any personal data processing through automated means with the help of, for example, a personal computer, a mobile device, or a router, is covered by both EU and CoE data protection rules.

Example: *Bodil Lindqvist*[197] concerned the reference to different persons by name or by other means such as their telephone number of information on their hobbies on an internet page. The CJEU held that "the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions or hobbies, constitutes the 'processing of personal data wholly or partly by automatic means'" within the meaning of Article 3 (1) of Directive 95/46.[198]

Example: In *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*,[199] Mr González requested the removal or alteration of a link between his name in the Google search engine and two newspaper pages announcing a real-estate auction for the recovery of social security debts. The CJEU stated that "in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of

195 General Data Protection Regulation, Art. 2 (1) and 4 (2).

196 Modernised Convention 108, Art. 2 (b) and (c); Explanatory Report of Modernised Convention 108, para. 21.

197 CJEU, C-101/01, *Criminal proceedings against Bodil Lindqvist*, 6 November 2003, para. 27.

198 General Data Protection Regulation, Art. 2 (1).

199 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 May 2014.

lists of search results".[200] The CJEU concluded that such actions constitute 'processing', "regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data".

2.2.3. Non-automated data processing

Manual data processing also requires data protection.

Data protection **under EU law** is in no way limited to automated data processing. Accordingly, under EU law, data protection applies to processing personal data in a manual filing system, that is, a specially structured paper file.[201] A structured filing system is one which categorises a set of personal data, making them accessible according to certain criteria. For example, if an employer maintains a paper file entitled 'employees leave', which contains all the details of leaves that staff have taken in the past year and is sorted in alphabetical order, the file will constitute a manual filing system subject to EU data protection rules. The reason for this extension of data protection is that:

- paper files can be structured in a way which makes finding information quick and easy;
- storing personal data in structured paper files makes it easy to circumvent the restrictions laid down by law for automated data processing.[202]

Under **CoE law**, the definition of automatic processing recognises that some stages of manual use of personal data may be required between automated operations.[203] Article 2 (c) of Modernised Convention 108 states that "(w)here automated processing is not used, data processing means an operation or set of operations performed upon personal data within a structured set of such data which is accessible or retrievable according to specific criteria".

200 *Ibid.*, para. 28.

201 General Data Protection Regulation, Art. 2 (1).

202 General Data Protection Regulation, Recital 15.

203 Modernised Convention 108, Art. 2 (b) and (c).

2.3. Users of personal data

Key points

- Whoever determines the means and purposes of processing the personal data of others is a 'controller' under data protection law; if several persons take this decision together, they may be 'joint controllers'.
- A 'processor' is a natural or legal person that processes personal data on behalf of a controller.
- A processor becomes a controller if it determines the means and purposes of data processing itself.
- Any person to whom personal data are disclosed is a 'recipient'.
- A 'third party' is a natural or legal person other than the data subject, the controller, the processor and persons who are authorised to process personal data under the direct authority of the controller or processor.
- Consent as a legal basis for processing personal data must be freely given, informed, specific and an unambiguous indication of wishes by a clear affirmative act signifying agreement to processing.
- Processing special categories of data on the basis of consent requires explicit consent.

2.3.1. Controllers and processors

The most important consequence of being a controller or a processor is legal responsibility for complying with the respective obligations under data protection law. In the private sector, this is usually a natural or legal person; in the public sector, it is usually an authority. There is a significant distinction between a data controller and a data processor: the former is the natural or legal person who determines the purposes and the means of processing, while the latter is the natural or legal person who processes the data on behalf of the controller, following strict instructions. In principle, it is the data controller that must exercise control over the processing and who has responsibility for this, including legal liability. However, with the reform of data protection rules, processors now have an obligation to comply with many of the requirements which apply to controllers. For example, under the GDPR, processors must maintain a record of all categories of processing activities to demonstrate compliance with their obligations under the regulation.[204] Processors are also required to

204 General Data Protection Regulation, Art. 30 (2).

implement appropriate technical and organisational measures to ensure the security of processing,[205] to appoint a Data Protection Officer in certain situations,[206] and to notify data breaches to the controller.[207]

Whether a person has the capacity to decide and determine the purpose and means of processing will depend on the factual elements or circumstances of the case. According to the definition of controller in the GDPR, natural persons, legal persons or any other bodies can be a controller. However, the Article 29 Working Party has emphasised that to provide individuals with a more stable entity for the exercise of their rights, "preference should be given to consider as controller the company or the body as such, rather than a specific person within the company or the body".[208] For example, a company selling healthcare supplies to practitioners is the controller of compiling and maintaining the distribution list of all practitioners in a certain area, and not the sales manager that actually uses and maintains the list.

Example: When the marketing division of the Sunshine company plans to process data for a market survey, the Sunshine company, not the employees of the marketing division, will be the controller of such processing. The marketing division cannot be the controller, as it has no separate identity.

Natural persons can be controllers under both EU and CoE law. However, when processing data about others regarding a purely personal or household activity, private individuals do not fall under the rules of the GDPR and Modernised Convention 108, and are not deemed to be controllers.[209] An individual who keeps his or her correspondence, a personal diary describing incidents with friends and colleagues and health records of family members, may be exempt from data protection rules, as these activities could be purely personal or merely household activities. The GDPR further specifies that personal or household activities could also include social networking and online activity when undertaken within the context of such activities.[210] To the contrary, data protection rules fully apply to controllers and processors who

205 *Ibid.*, Art. 32.

206 *Ibid.*, Art. 37.

207 *Ibid.*, Art. 33 (2).

208 Article 29 Working Party (2010), *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP 169, Brussels, 16 February 2010.

209 General Data Protection Regulation, Recital 18 and Art. 2 (2) (c); Modernised Convention 108, Art. 3 (2).

210 General Data Protection Regulation, Recital 18.

provide the means for processing personal data for personal or household activities (for example, social networking platforms).[211]

Citizens' access to the internet and the possibility to use e-commerce platforms, social networks and blogging sites to share personal information about themselves and other individuals make it increasingly difficult to separate personal from non-personal processing.[212] Whether activities are purely personal or household depends on the circumstances.[213] Activities that have professional or commercial aspects cannot fall under the household exemption.[214] Thus, where the scale and frequency of data processing suggests a professional or full-time activity, a private individual could be considered as controller. In addition to the professional or commercial character of the processing activity, another factor that must be taken into account is whether personal data are made available to a large number of persons, obviously external to the private sphere of the individual. Case law under the Data Protection Directive has found that data protection law will apply when a private person, in the course of using the internet, publishes data about others on a public website. The CJEU has not yet ruled on similar facts under the GDPR, which provides more guidance on the topics that could be considered outside the scope of the data protection legislation under the 'household exception', such as use of social media for personal purposes.

Example: *Bodil Lindqvist*[215] concerned the reference to different persons by name or by other means, such as their telephone number or information on their hobbies, on an internet page. The CJEU maintained that "the act of referring, on an internet page, to various persons and identifying them by name or by other means [...] constitutes 'the processing of personal data wholly or partly by automatic means'" within the meaning of Article 3 (1) of the Data Protection Directive.[216]

211 *Ibid*., Recital 18; Explanatory Report of Modernised Convention 108, para. 29.

212 See the statement of Article 29 Working Party on discussions regarding the data protection reform package (2013), *Annex 2 : Proposals and Amendments regarding exemption for personal or household activities*, 27 February 2013.

213 Explanatory Report of Modernised Convention 108, para. 28.

214 See General Data Protection Regulation, Recital 18 and Explanatory Report of Modernised Convention 108, para. 27.

215 CJEU, C-101/01, *Criminal proceedings against Bodil Lindqvist*, 6 November 2003.

216 *Ibid*., para. 27; Former Directive 95/46/EC, Art. 3 (1), now General Data Protection Regulation, Art. 2 (1).

Such personal data processing does not fall under purely personal or domestic activities, which are outside the scope of EU data protection rules, as this exception "must [...] be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people."[217]

According to the CJEU, the visual recordings of a privately installed security camera can also be covered by EU data protection legislation under certain circumstances.

Example: In *František Ryneš*,[218] Mr Ryneš captured the image of two individuals who broke windows in his home through the domestic CCTV surveillance system he had installed to protect his property. The recording was then handed over to the police and relied on during criminal proceedings.

The CJEU stated that "[t]o the extent that video surveillance [...] covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely 'personal or household' [...]." [219]

Controller

Under EU law, a controller is defined as someone who "alone or jointly with others determines the purposes and means of the processing of personal data".[220] A controller's decision establishes why and how data shall be processed.

Under CoE law, Modernised Convention 108 defines a 'controller' as "the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has the decision-making power with respect to data processing".[221] Such decision-making power concerns the purposes and means of

217 CJEU, C-101/01, *Criminal proceedings against Bodil Lindqvist*, 6 November 2003, para. 47.

218 CJEU, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, 11 December 2014, para. 33.

219 Former Directive 95/46/EC, Art. 3 (2) second indent, now General Data Protection Regulation, Art. 2 (2) (c).

220 General Data Protection Regulation, Art. 4 (7).

221 Modernised Convention 108, Art. 2 (d).

the processing, as well as the data categories to be processed and access to the data.[222] Whether this power derives from a legal designation or from factual circumstances must be decided on a case-by-case basis.[223]

Example: *Google Spain*[224] was brought by a Spanish citizen who wanted to have an old newspaper report on his financial history removed from Google.

The CJEU was asked whether Google, as the operator of a search engine, was the 'controller' of the data within the meaning of Article 2 (d) of the Data Protection Directive.[225] The CJEU considered a broad definition of the notion 'controller' to ensure "effective and complete protection of data subjects".[226] The CJEU found that the search engine operator determined the purposes and means of the activity and that it rendered data loaded on internet pages by publishers of websites accessible to any internet user who carries out a search on the basis of the data subject's name.[227] Therefore, the CJEU determined that Google can be regarded as the 'controller'.[228]

When a controller or processor is established outside of the EU, that company needs to appoint, in writing, a representative within the EU.[229] The GDPR underlines that the representative must be established "in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods and services to them, or whose behaviour is monitored".[230] If no representative is designated, legal action can still be initiated against the controller or the processor themselves.[231]

222 Explanatory Report of Modernised Convention 108, para. 22.

223 *Ibid.*

224 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 May 2014.

225 General Data Protection Regulation, Art. 4 (7); CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 May 2014, para. 21.

226 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 May 2014, para. 34.

227 *Ibid.*, paras. 35–40.

228 *Ibid.*, para. 41.

229 General Data Protection Regulation, Art. 27 (1).

230 *Ibid.*, Art. 27 (3).

231 *Ibid.*, Art. 27 (5).

Joint controllership

The GDPR provides that where two or more controllers jointly determine the purpose and means of processing, they are considered joint controllers. This means that they decide together to process data for a shared purpose.[232] The Explanatory Report of Modernised Convention 108 states that multiple controllers or co-controllership is also possible within **the CoE framework**.[233]

The Article 29 Working Party points out that joint controllership may take different forms, and that participation of the different controllers in the control activities may be unequal.[234] Such flexibility makes it possible to cater for increasingly complex data processing realities.[235] Joint controllers must therefore determine their respective responsibilities for compliance with the obligations under the regulation in a specific agreement.[236]

Joint controllership leads to joint responsibility for a processing activity.[237] Within the framework of **EU law**, this means that each controller or processor can be held fully liable for the entire damage caused by processing under joint controllership, to ensure that the data subject is effectively compensated.[238]

> Example: A database run jointly by several credit institutions on their defaulting customers is a common example of joint controllership. When someone applies for a credit line from a bank that is one of the joint controllers, the banks check the database to help them make informed decisions about the applicant's creditworthiness.

Legal provisions do not explicitly state whether joint controllership requires the shared purpose to be the same for each of the controllers or whether it is sufficient if their purposes only partly overlap. As of yet, no relevant case law is available at the European level. In its 2010 Opinion on controllers and processors, the Article 29

232 *Ibid.*, Art. 4 (7) and Art. 26.

233 Modernised Convention 108, Art. 2 (d); Explanatory Report of Modernised Convention 108, para. 22.

234 Article 29 Working Party (2010), *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP 169, Brussels, 16 February 2010, p. 19.

235 *Ibid.*

236 General Data Protection Regulation, Recital 79.

237 *Ibid.*, para. 21.

238 *Ibid.*, Art. 82 (4).

Working Party states that joint controllers may either share all purposes and means of processing or they may share only some purposes or means or part thereof.[239] Whereas the former would imply a very close relationship between the different actors, the latter would indicate a looser relationship.

The Article 29 Working Party advocates a broader interpretation of the concept of joint controllership with the aim of allowing some flexibility to cater for the increasing complexity of current data processing reality.[240] A case involving the Society for Worldwide Interbank Financial Telecommunication (SWIFT) illustrates the Working Party's position.

Example: In the so-called SWIFT case, European banking institutions employed SWIFT, initially as a processor, to operate data transfer in the course of banking transactions. SWIFT disclosed such banking transaction data, stored in a computing service centre in the United States (US), to the US Treasury Department without being explicitly ordered to do so by the European banking institutions that employed it. The Article 29 Working Party, when evaluating the lawfulness of this situation, came to the conclusion that the European banking institutions employing SWIFT, as well as SWIFT itself, had to be seen as joint controllers responsible to European customers for the disclosure of their data to the US authorities.[241]

Processor

A processor is defined **under EU law** as someone who processes personal data on behalf of a controller.[242] The activities entrusted to a processor may be limited to a very specific task or context or may be quite general and comprehensive.

Under CoE law, the meaning of a processor is the same as under EU law.[243]

239 Article 29 Working Party (2010), *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP 169, Brussels, 16 February 2010, p. 19.

240 *Ibid*.

241 Article 29 Working Party (2006), *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT),* WP 128, Brussels, 22 November 2006.

242 General Data Protection Regulation, Art. 4 (8).

243 Modernised Convention 108, Art. 2 (f).

Processors, besides processing data for others, will also be data controllers in their own right in relation to the processing they perform for their own purposes, for example, the administration of their own employees, sales and accounts.

Example: The Everready company specialises in data processing for the administration of human resource data for other companies. In this function, Everready is a processor. Where Everready processes the data of its own employees, however, it is the controller of data processing operations for the purpose of fulfilling its obligations as an employer.

Relationship between controller and processor

As we have seen, the controller is defined as the one who determines the purposes and the means of processing. The GDPR clearly states that the processor may only process personal data on instructions from the controller, unless the EU or Member State law requires the processor to do so.[244] The contract between the controller and the processor is an essential element of their relationship, and is a legal requirement.[245]

Example: The director of the Sunshine Company decides that the Cloudy Company – a specialist in cloud-based data storage – should manage Sunshine's customer data. The Sunshine Company remains the controller and Cloudy Company is only a processor, as, according to the contract, Cloudy may only use Sunshine company's customer data for the purposes that Sunshine determines.

If the power to determine the means of processing is delegated to a processor, the controller must nonetheless be able to exercise an appropriate degree of control over the processor's decisions regarding the means of processing. Overall responsibility still lies with the controller, who must supervise the processors to ensure that their decisions comply with data protection law and with its own instructions.

Furthermore, should a processor not respect the conditions for data processing as prescribed by the controller, the processor will have become a controller at least to

244 General Data Protection Regulation, Art. 29.

245 *Ibid.*, Art. 28 (3).

the extent of the breach of the controller's instructions. This will most likely make the processor a controller who acts unlawfully. In turn, the initial controller will have to explain how it was possible for the processor to breach its mandate.[246] Indeed, the Article 29 Working Party tends to presume joint controllership in such cases, since this results in the best protection of the data subjects' interests.[247]

There may also be issues about the division of responsibility where a controller is a small enterprise and the processor is a large corporate company which has the power to dictate the conditions of its services. In such circumstances, however, the Article 29 Working Party maintains that the standard of responsibility should not be lowered on the ground of economic imbalance and that the understanding of the concept of controller must be maintained.[248]

For the sake of clarity and transparency, the details of the relationship between a controller and a processor must be recorded in a written contract.[249] The contact must include in particular the subject matter, nature, purpose and duration of the processing, the type of personal data and the categories of data subjects. It should also stipulate the controller's and the processor's obligations and rights, such as requirements regarding confidentiality and security. Having no such contract is an infringement of the controller's obligation to provide written documentation of mutual responsibilities, and could lead to sanctions. When damage is caused as a result of acting outside or failing to comply with the controller's lawful instructions, it is not just the controller who can be held liable, but also the processor.[250] The processor must keep records of all categories of processing activities it carries out on behalf of the controller.[251] These records must be made available to the supervisory authority at its request, as the controller and the processor must both cooperate with that authority in the performance of its tasks.[252] Controllers and processors also have the

246 *Ibid*., Art. 82 (2).

247 Article 29 Working Party (2010), *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP 169, Brussels, 16 February 2010, p. 25; Article 29 Working Party (2006), *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, WP 128, Brussels, 22 November 2006.

248 Article 29 Working Party (2010), *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP 169, Brussels, 16 February 2010, p. 26.

249 General Data Protection Regulation, Art. 28 (3) and (9).

250 *Ibid*., Art. 82 (2).

251 *Ibid*., Art. 30 (2).

252 *Ibid.,* Art. 30 (4) and 31.

possibility of adhering to an approved code of conduct or a certification mechanism to demonstrate their compliance with the GDPR requirements.[253]

Processors might want to delegate certain tasks to additional sub-processors. This is legally permissible, providing appropriate contractual stipulations are established between the controller and the processor, including whether the controller's authorisation is necessary in every single case or whether informing alone is sufficient. The GDPR stipulates that the initial processor remains fully liable to the controller where a sub-processor fails to fulfil its data protection obligations.[254]

Under CoE law, the interpretation of the concepts of controller and processor, as explained above, is fully applicable.[255]

2.3.2. Recipients and third parties

The difference between these two categories of persons or entities, which were introduced by the Data Protection Directive, lies mainly in their relationship to the controller and, consequently, in their authorisation to access personal data held by the controller.

A 'third party' is someone who is different from the controller and the processor. According to Article 4 (10) of the GDPR, a third party is "a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data". This means that persons working for an organisation which is different from the controller – even if it belongs to the same group or holding company – will be (or belong to a) 'third party'. On the other hand, branches of a bank processing customer's accounts under the direct authority of their headquarters would not be 'third parties'.[256]

'Recipient' is a broader term than 'third party'. In the meaning of Article 4 (9) of the GDPR, a recipient means "a natural or legal person, public authority, agency or another body, to which data are disclosed, whether a third party or not". This recipient may either be a person outside the controller or processor – this would then be a

253 *Ibid.*, Art. 28 (5) and 42 (4).

254 *Ibid.*, Art. 28 (4).

255 See, for example, Modernised Convention 108, Art. 2 (b) and (f); Profiling Recommendation, Art. 1.

256 Article 29 Working Party (2010), *Opinion 1/2010 on the concept of "controller" and "processor"*, WP 169, Brussels, 16 February 2010, p. 31.

third party – or someone inside the controller or processor, such as an employee or another division within the same company or authority.

The distinction between recipients and third parties is important only because of the conditions for lawful disclosure of data. The employees of a controller or processor may be recipients of personal data without further legal requirement if they are involved in the processing operations of the controller or processor. Whereas, a third party, being separate from the controller or processor, is not authorised to use the personal data a controller processes, unless on specific legal grounds in a specific case.

Example: A controller's employee, who uses personal data within the remit of tasks the employer entrusted to him or her, is a recipient of data, but not a third party, as he or she uses the data in the name and under the instructions of the controller. For example, if an employer discloses personal data on its employees to its human resources department in view of upcoming performance evaluations, the human resources team will be recipients of personal data, as the data have been disclosed to them in the course of processing for the controller.

If, however, the organisation provides data on its employees to a training company which will use it to tailor a training program for the employees, the training company is a third party. The reason is that the training company does not have specific legitimacy or authorisation (which in the "human resources" case stems from the employment relationship with the controller) to process these personal data. In other words, they have not received the information in the course of their employment with the data controller.

2.4. Consent

Key points

- Consent as a legal basis for processing personal data must be freely given, informed, specific and an unambiguous indication of wishes by a clear affirmative act signifying agreement to processing.
- Processing special categories of data requires explicit consent.

As will be considered in detail in Chapter 4, consent is one of the six legitimate grounds for processing personal data. Consent means "any freely given, specific, informed and unambiguous indication of the data subject's wishes."[257]

EU law sets out several elements for consent to be valid, which aim to guarantee that data subjects truly meant to agree to a particular use of their data:[258]

- Consent must be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of his or her personal data. Such an act may be an action or a statement.

- The data subject must have the right to withdraw consent at any time.

- Within the context of a written declaration that also covers other matters, such as 'terms of service', requests for consent must be in clear and plain language and in an intelligible and easily accessible form, which clearly distinguishes consent from other matters; if a part of this declaration violates the GDPR it shall not be binding.

Consent will only be valid in the context of data protection law if all of these requirements are fulfilled. It is the controller's responsibility to demonstrate that the data subject consented to the processing of his or her data.[259] The elements of valid consent will be discussed further in Section 4.1.1 on lawful grounds for processing personal data.

Convention 108 does not contain a definition for consent; this is left to domestic law. However, **under CoE law**, the elements of valid consent correspond to those explained earlier.[260]

Additional requirements under civil law for valid consent, such as legal capacity, naturally apply also in the context of data protection, as such requirements are fundamental legal prerequisites. Invalid consent of persons who do not have legal capacity will result in the absence of a legal basis for processing data about such persons.

257 General Data Protection Regulation, Art. 4 (11). See also Modernised Convention 108, Art. 5 (2).

258 General Data Protection Regulation, Art. 7.

259 *Ibid.*, Art. 7 (1).

260 Modernised Convention 108, Art. 5 (2); Explanatory Report of Modernised Convention 108, paras. 42–45.

Concerning the legal capacity of minors to enter contracts, the GDPR provides that its rules on the minimum age to obtain valid consent do not affect the general contract law of Member States.[261]

Consent must be given in a clear manner so as to leave no doubt about the intention of the data subject.[262] Consent must be explicit when it concerns the processing of sensitive data, and can be done orally or in writing.[263] The latter can be done by electronic means.[264] Within the framework of both **EU** and **CoE law**, agreement to the processing of one's personal data must be given by a statement or by a clear affirmative action.[265] Thus, consent cannot be derived from silence, pre-ticked boxes, pre-completed forms or inactivity.[266]

261 General Data Protection Regulation, Art. 8 (3).

262 *Ibid*., Art. 6 (1) (a) and 9 (2) (a).

263 *Ibid*., Recital 32.

264 *Ibid*.

265 *Ibid*., Art. 4 (11); Explanatory Report of Modernised Convention 108, para. 42.

266 General Data Protection Regulation, Recital 32; Explanatory Report of Modernised Convention 108, para. 42.

3

Key principles of European data protection law

EU	Issues covered	CoE
General Data Protection Regulation, Article 5 (1) (a)	**The lawfulness principle**	Modernised Convention 108, Article 5 (3)
General Data Protection Regulation, Article 5 (1) (a)	**The fairness principle**	Modernised Convention 108, Article 5 (4) (a) ECtHR, *K.H. and Others v. Slovakia*, No. 32881/04, 2009
General Data Protection Regulation, Article 5 (1) (a) CJEU, C-201/14, *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others*, 2015	**The transparency principle**	Modernised Convention 108, Article 5 (4) (a) and Article 8 ECtHR, *Haralambie v. Romania*, No. 21737/03, 2009
General Data Protection Regulation, Article 5 (1) (b)	**The purpose limitation principle**	Modernised Convention 108, Article 5 (4) (b)
General Data Protection Regulation, Article 5 (1) (c) CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Kärntner Landesregierung and Others* [GC], 2014	**The data minimisation principle**	Modernised Convention 108, Article 5 (4) (c)
General Data Protection Regulation, Article 5 (1) (d) CJEU, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*, 2009	**The data accuracy principle**	Modernised Convention 108, Article 5 (4) (d)

EU	Issues covered	CoE
General Data Protection Regulation, Article 5 (1) (e) CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Kärntner Landesregierung and Others* [GC], 2014	**The storage limitation principle**	Modernised Convention 108, Article 5 (4) (e) ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 2008
General Data Protection Regulation, Articles 5 (1) (f) and 32	**The data security (integrity and confidentiality) principle**	Modernised Convention 108, Article 7
General Data Protection Regulation, Article 5 (2)	**The accountability principle**	Modernised Convention 108, Article 10

Article 5 of the General Data Protection Regulation sets out the principles governing the processing of personal data. These principles cover:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- data accuracy;
- storage limitation;
- integrity and confidentiality.

The principles serve as the starting point for more detailed provisions in the subsequent articles of the regulation. They appear also in Articles 5, 7, 8 and 10 of Modernised Convention 108. All later data protection legislation at the CoE or EU level must comply with these principles and they must be kept in mind when interpreting such legislation. Under EU law, restrictions to processing principles are only allowed to the extent that they correspond to rights and obligations provided for in Articles 12 to 22 and they must respect the essence of the fundamental rights and freedoms. Any exemptions from and restrictions to these key principles may be provided for at EU or national level;[267] they must be provided for by law, pursue a legitimate aim and be necessary and proportionate measures in a democratic society. [268] All three conditions must be fulfilled.

267 Modernised Convention 108, Art. 11 (1); General Data Protection Regulation, Art. 23 (1).

268 General Data Protection Regulation, Art. 23 (1).

3.1. The lawfulness, fairness and transparency of processing principles

Key points

- The principles of lawfulness, fairness and transparency apply to all personal data processing.
- Under the GDPR, lawfulness requires either:
  - consent of the data subject;
  - necessity to enter a contract;
  - a legal obligation;
  - necessity to protect the vital interests of the data subject or of another person;
  - necessity for performing a task in the public interest;
  - necessity for the legitimate interests of the controller or a third party, if they are not overridden by the interests and rights of the data subject.
- Personal data processing should be done in a fair manner.
  - The data subject must be informed of the risk to ensure that processing does not have unforeseeable negative effects.
- Personal data processing should be done in a transparent manner.
  - Controllers must inform data subjects before processing their data, among other details, about the purpose of processing and about the identity and address of the controller.
  - Information on processing operations must be provided in clear and plain language to allow data subjects to easily understand the rules, risks, safeguards and rights involved.
  - Data subjects have the right to access their data wherever they are processed.

3.1.1. Lawfulness of processing

EU and CoE data protection laws require personal data to be processed lawfully.[269] Lawful processing requires the consent of the data subject or another legitimate

269 Modernised Convention 108, Art. 5 (3); General Data Protection Regulation, Art. 5 (1) (a).

ground provided in the data protection legislation.[270] Article 6 (1) of the GDPR includes five lawful grounds for processing, in addition to consent, i.e. when processing personal data is necessary for the performance of a contract, for the performance of a task carried out in the exercise of public authority, for compliance with a legal obligation, for the purpose of the legitimate interests of the controller or third parties, or if necessary to protect the vital interests of the data subject. This will be discussed in more detail in Section 4.1.

3.1.2. Fairness of processing

In addition to lawful processing, EU and CoE data protection laws require personal data to be processed fairly.[271] The principle of fair processing governs primarily the relationship between the controller and the data subject.

Controllers should notify data subjects and the general public that they will process data in a lawful and transparent manner and must be able to demonstrate the compliance of processing operations with the GDPR. Processing operations must not be performed in secret and data subjects should be aware of potential risks. Furthermore, controllers, so far as possible, must act in a way which promptly complies with the wishes of the data subject, especially where his or her consent forms the legal basis for the data processing.

Example: In *K.H. and Others v. Slovakia*,[272] the applicants – women of Roma ethnic origin – had been treated in two hospitals in eastern Slovakia during their pregnancies and deliveries. Afterwards, none of them were able to conceive a child again despite repeated attempts. The national courts ordered the hospitals to permit the applicants and their representatives to consult and make handwritten excerpts of the medical records but dismissed their request to photocopy the documents, allegedly with a view to preventing their abuse. The states' positive obligations under Article 8 of the ECHR necessarily included an obligation to make available to the data subject copies of his or her data files. It was for the state to determine the arrangements for copying personal data files, or, where appropriate, to show

270 Charter of Fundamental Rights of the European Union, Art. 8 (2); General Data Protection Regulation, Recital 40 and Art. 6–9; Modernised Convention 108, Art. 5 (2); Explanatory Report of Modernised Convention 108, para. 41.

271 General Data Protection Regulation, Art. 5 (1) (a); Modernised Convention 108, Art. 5 (4) (a).

272 ECtHR, *K.H. and Others v. Slovakia*, No. 32881/04, 28 April 2009.

compelling reasons for refusing to do so. In the applicants' case, the domestic courts justified prohibiting the applicants from making copies of their medical records principally on the need to protect the relevant information from abuse. However, the ECtHR failed to see how the applicants, who had in any event been given access to their entire medical files, could have abused information concerning themselves. Moreover, the risk of such abuse could have been prevented by means other than denying copies of the files to the applicants, such as by limiting the range of persons entitled to access the files. The state failed to show the existence of sufficiently compelling reasons to deny the applicants effective access to information concerning their health. The Court concluded that there had been a violation of Article 8.

In relation to internet services, the features of data processing systems must make it possible for data subjects to really understand what is happening with their data. In any case, the principle of fairness goes beyond transparency obligations and could also be linked to processing personal data in an ethical manner.

Example: A university research department conducts an experiment analysing changes of mood on 50 subjects. These are required to register in an electronic file their thoughts every hour, at a given time. The 50 persons gave their consent for this particular project, and this specific use of the data by the university. The research department soon discovers that electronically logging thoughts would be very useful for another project focused on mental health, under the coordination of another team. Even though the university, as controller, could have used the same data for the work of another team without further steps to ensure lawfulness of processing that data, given that the purposes are compatible, the university informed the subjects and asked for new consent, following its research ethics code and the principle of fair processing.

3.1.3. Transparency of processing

EU and CoE data protection laws require personal data processing to be done "in a transparent manner in relation to the data subject".[273]

273 General Data Protection Regulation, Art. 5 (1) (a); Modernised Convention 108, Art. 5 (4) (a) and 8.

This principle establishes an obligation for the controller to take any appropriate measure in order to keep the data subjects – who may be users, customers or clients – informed about how their data are being used.[274] Transparency may refer to the information given to the individual before the processing starts,[275] the information that should be readily accessible to data subjects during the processing,[276] but also to the information given to data subjects following a request of access to their own data.[277]

> Example: In the case of *Haralambie v. Romania*,[278] the applicant was only granted access to the information held on him by the secret service organisation five years after his request. The ECtHR reiterated that individuals who were the subject of personal files held by public authorities had a vital interest in being able to access them. The authorities had a duty to provide an effective procedure for obtaining access to such information. The ECtHR considered that neither the quantity of the files transmitted nor shortcomings in the archive system justified a delay of five years in granting the applicant's request for access to his files. The authorities had not provided the applicant with an effective and accessible procedure to enable him to obtain access to his personal files within a reasonable time. The Court concluded that there had been a violation of Article 8 of the ECHR.

Processing operations must be explained to the data subjects in an easily accessible way which ensures that they understand what will happen to their data. This means that the specific purpose of processing personal data must be known by the data subject at the time of the collection of the personal data.[279] The transparency of processing requires that clear and plain language be used.[280] It must be clear to the people concerned what are the risks, rules, safeguards and rights regarding the processing of their personal data.[281]

274 General Data Protection Regulation, Art. 12.

275 *Ibid.,* Art. 13 and 14.

276 Article 29 Working Party, *Opinion 2/2017 on data processing at work*, p. 23.

277 General Data Protection Regulation, Art. 15.

278 ECtHR, *Haralambie v. Romania*, No. 21737/03, 27 October 2009.

279 General Data Protection Regulation, Recital 39.

280 *Ibid.*

281 *Ibid.*

CoE law also specifies that certain essential information has to be compulsorily provided in a proactive manner by the controller to the data subjects. Information on the name and address of the controller (or co-controllers), the legal basis and the purposes of the data processing, the categories of data processed and recipients, as well as the means of exercising the rights can be provided in any appropriate format (either through a website, technological tools on personal devices, etc.) as long as the information is fairly and effectively presented to the data subject. The information presented should be easily accessible, legible, understandable and adapted to the relevant data subjects (in a child friendly language where necessary for instance). Any additional information that is necessary to ensure fair data processing or that is useful for such purpose, such as the preservation period, the knowledge of the reasoning underlying the data processing, or information on data transfers to a recipient in another Party or non-Party (including whether that particular non-Party provides an appropriate level of protection or the measures taken by the controller to guarantee such an appropriate level of data protection) is also to be provided.[282]

Pursuant to the right of access,[283] a data subject has the right to be told by a controller at his/her request if his/her data are being processed, and, if so, which data are subject to such processing.[284] Additionally, pursuant to the right to information,[285] the persons whose data are processed must be informed by controllers or processors pro-actively about the purposes, length, means of processing, among other details, in principle before the processing activity starts.

Example: The case *Smaranda Bara and Others v. Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală (ANAF)*[286] concerned the transmission of tax data relating to the income of self-employed persons from the National Tax Administration Agency to the National Health Insurance Fund in Romania, on the basis of which the payment of arrears of health insurance contributions were required. The CJEU was asked to determine whether prior information should have been given to the data subject regarding the identity of the data controller and the purpose

282 Explanatory Report of Modernised Convention 108, para. 68.

283 General Data Protection Regulation, Art. 15.

284 Modernised Convention 108, Art. 8 and 9 (1) (b).

285 General Data Protection Regulation, Art. 13 and 14.

286 CJEU, C-201/14, *Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others*, 1 October 2015, paras. 28–46.

for transmitting the data before these data were processed by the National Health Insurance Fund. The CJEU held that where a public administrative body of a Member State transmits personal data to another public administrative body that further processes those data, the data subjects must be informed about that transmission or processing.

In certain situations, derogations are allowed from the obligation to inform data subjects about data processing, and these will be discussed in more detail in Section 6.1 on the rights of the data subject.

3.2. The principle of purpose limitation

Key points

- The purpose of processing data must be defined before processing is started.
- There can be no further processing of data in a way that is incompatible with the original purpose, though the General Data Protection Regulation foresees exceptions to this rule for archiving purposes in the public interest, scientific or historical research purposes and statistical purposes.
- In essence, the principle of purpose limitation means that any processing of personal data must be done for a specific well-defined purpose and only for additional, specified, purposes that are compatible with the original one.

The principle of purpose limitation is one of the fundamental principles of European data protection law. It is strongly connected with transparency, predictability and user control: if the purpose of processing is sufficiently specific and clear, individuals know what to expect and transparency and legal certainty are enhanced. At the same time, clear delineation of the purpose is important to enable data subjects to effectively exercise their rights, such as the right to object to processing.[287]

The principle requires that any processing of personal data must be done for a specific, well-defined purpose and only for additional purposes that are compatible with the original purpose.[288] The processing of personal data for undefined and/or unlimited purposes is thus unlawful. The processing of personal data without a certain

287 Article 29 Working Party (2013), *Opinion 3/2013 on purpose limitation*, WP 203, 2 April 2013.

288 General Data Protection Regulation, Art. 5 (1) (b).

purpose, just based on the consideration they may be useful sometime in the future, is also not lawful. The legitimacy of processing personal data will depend on the purpose of the processing, which must be explicit, specified and legitimate.

Every new purpose for processing data which is not compatible with the original one must have its own particular legal basis and cannot rely on the fact that the data were initially acquired or processed for another legitimate purpose. In turn, legitimate processing is limited to its initially specified purpose and any new purpose of processing will require a separate new legal basis. For instance, disclosure of personal data to third parties for a new purpose will have to be carefully considered, as such disclosure will likely need an additional legal basis, distinct from the one for collecting the data.

Example: An airline collects data from its passengers to make bookings to operate the flight properly. The airline will need data on: passengers' seat numbers; special physical limitations, such as wheelchair needs; and special food requirements, such as kosher or halal food. If airlines are asked to transmit these data, which are contained in the Passenger Name Record, to the immigration authorities at the port of landing, these data are then being used for immigration control purposes, which differ from the initial data collection purpose. Transmission of these data to an immigration authority will therefore require a new and separate legal basis.

When considering the scope and limits of a particular purpose, Modernised Convention 108 and the General Data Protection Regulation rely on the concept of compatibility: the use of data for compatible purposes is allowed on the grounds of the initial legal basis. Further processing of the data may not, therefore, be done in a way that is unexpected, inappropriate or objectionable for the data subject.[289] To assess whether the further processing is to be considered compatible, the controller should take the following into account (among others things):

- "any link between those purposes and the purposes of the intended further processing;

- the context in which the personal data have been collected, in particular concerning the reasonable expectations of data subjects based on their relationship with the controller on its further use;

289 Explanatory Report of Modernised Convention 108, para. 49.

- the nature of the personal data;
- the consequences of the intended further processing for data subjects; and
- the existence of appropriate safeguards in both the original and intended further processing operations."[290] This could be done, for instance, through encryption or pseudonymisation.

Example: The Sunshine company acquires customer data in the course of customer relations management (CRM). It then transmits these data to a direct marketing company, the Moonlight company, which wants to use these data to assist the marketing campaigns of third companies. Sunshine's transmission of data for marketing by other companies constitutes a subsequent use of data for a new purpose, which is incompatible with CRM, the Sunshine company's initial purpose for collecting the customer data. The transmission of the data to the Moonlight company therefore needs its own legal basis.

By contrast, the Sunshine company's use of CRM data for its own marketing purposes, that is sending marketing messages to its own customers for its own products, is generally accepted as a compatible purpose.

The General Data Protection Regulation and Modernised Convention 108 declare that the "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" is *a priori* considered compatible with the initial purpose.[291] However, appropriate safeguards such as the anonymisation, encryption or pseudonymisation of the data, and restriction of access to the data, must be put in place when further processing personal data.[292] The General Data Protection Regulation adds that "[w]here the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in

290 General Data Protection Regulation, Recital 50 and Art. 6 (4); Explanatory Report of Modernised Convention 108, para. 49.

291 General Data Protection Regulation, Art. 5 (1) (b); Modernised Convention 108, Art. 5 (4) (b). An example of such national provisions is the Austrian Data Protection Act (*Datenschutzgesetz*), Federal Law Gazette I No. 165/1999, para. 46.

292 General Data Protection Regulation Art. 6 (4); Modernised Convention 108, Art. 5 (4) (b); Explanatory Report of Modernised Convention 108, para. 50.

particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes".[293] When undertaking further processing, the data subject should therefore be informed of the purposes, as well as of his or her rights, such as the right to object.[294]

Example: The Sunshine company has collected and stored Customer Relations Management (CRM) data about its customers. Further use of these data by the Sunshine company for a statistical analysis of the buying behaviour of its customers is permissible, as statistics are a compatible purpose. No additional legal basis, such as consent of the data subjects, is needed. However, for the further processing of the personal data for statistical purposes, the Sunshine company must put in place appropriate safeguards for the rights and freedoms of the data subject. The technical and organisational measures that Sunshine must implement may include pseudonymisation.

3.3. The data minimisation principle

Key points

- Data processing must be limited to what is necessary to fulfil a legitimate purpose.
- The processing of personal data should only take place when the purpose of the processing cannot be reasonably fulfilled by other means.
- Data processing may not disproportionately interfere with the interests, rights and freedoms at stake.

Only such data shall be processed as are "adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed".[295] The categories of data chosen for processing must be necessary in order to achieve the declared overall aim of the processing operations, and a controller should strictly limit collection of data to such information as is directly relevant for the specific purpose pursued by the processing.

293 General Data Protection Regulation, Recital 50.

294 *Ibid*.

295 Modernised Convention 108, Art. 5 (4) (c); General Data Protection Regulation, Art. 5 (1) (c).

Example: In the *Digital Rights Ireland* case,[296] the CJEU considered the validity of the Data Retention Directive, which aimed to harmonise national provisions for retaining personal data generated or processed by publicly available electronic communications services or networks for their possible transmission to competent authorities to fight serious crime, such as organised crime and terrorism. Notwithstanding that this was considered a purpose that genuinely satisfies an objective of general interest, the generalised way in which the Directive covered "all individuals and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime", was considered problematic.[297]

Furthermore, by making use of special privacy-enhancing technology, it is sometimes possible to avoid using personal data at all, or to use measures to reduce the ability to attribute data to a data subject (for instance, through pseudonymisation), which results in a privacy-friendly solution. This is particularly appropriate in more extensive processing systems.

Example: A town council offers a chip card to regular users of the town's public transport system for a certain fee. The card carries the name of the user in written form on the card's surface and also in electronic form in the chip. Whenever a bus or tram is used, the chip card must be passed in front of the reading devices installed, for example, in buses and trams. The data read by the device are electronically checked against a database containing the names of the people who have bought the travel card.

This system does not adhere to the data minimisation principle in an optimal way: checking whether an individual is allowed to use transport facilities could be accommodated without comparing the personal data on the card's chip with a database. It would suffice, for instance, to have a special electronic image, such as a bar code, in the chip of the card which, upon being passed in front of the reading device, would confirm whether the card is valid or not. Such a system would not record who used which transport facility at what time. This would be the optimal solution in the sense of the

296 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [GC], 8 April 2014.

297 *Ibid.*, paras. 44 and 57.

minimisation principle, as this principle results in the obligation to minimise data collection.

Article 5 (1) of Modernised Convention 108 contains a proportionality requirement for processing personal data in relation to the legitimate purpose pursued. There must be a fair balance between all interests concerned at all stages of the processing. This means that "[p]ersonal data which is adequate and relevant but would entail a disproportionate interference in the fundamental rights and freedoms at stake should be considered as excessive".[298]

3.4. The data accuracy principle

Key points

- The principle of data accuracy must be implemented by the controller in all processing operations.
- Inaccurate data must be erased or rectified without delay.
- Data may need to be checked regularly and kept up to date to secure accuracy.

A controller holding personal information shall not use that information without taking steps to ensure with reasonable certainty that the data are accurate and up to date.[299]

The obligation to ensure accuracy of data must be seen in the context of the purpose of data processing.

Example: In the *Rijkeboer* case,[300] the CJEU considered the request of a Dutch national to receive information from the local administration of the city of Amsterdam on the identity of the persons to whom the records on him held by the local authority had been communicated in the two preceding years,

298 Explanatory Report of Modernised Convention 108, para. 52; General Data Protection Regulation, Art. 5 (1) (c).

299 General Data Protection Regulation, Art. 5 (1) (d); Modernised Convention 108, Art. 5 (4) (d).

300 CJEU, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*, 7 May 2009.

and also on the content of the disclosed data. The CJEU stated that the "right to privacy means that the data subject may be certain that his personal data are processed in a correct and lawful manner, that is to say, in particular, that the basic data regarding him are accurate and that they are disclosed to authorised recipients." The CJEU then referred to the preamble of the Data Protection Directive, which states that data subjects must enjoy the right of access to their personal data in order to be able to check that the data are correct.[301]

There may also be cases where updating stored data is legally prohibited, because the purpose of storing the data is principally to document events as a historical 'snap-shot'.

Example: A medical record of an operation must not be changed, in other words 'updated', even if findings mentioned in the record later on turn out to have been wrong. In such circumstances, only additions to the remarks in the record may be made, as long as they are clearly marked as contributions made at a later stage.

On the other hand, there are situations where it is absolute necessity to update and regularly check the accuracy of data, due to the potential damage which might be caused to the data subject if data were to remain inaccurate.

Example: If somebody wants to conclude a credit contract with a banking institution, the bank will usually check the creditworthiness of the prospective customer. For this purpose, there are special databases available containing data on the credit history of private individuals. If such a database provides incorrect or outdated data about an individual, this person may suffer negative effects. Controllers of such databases must therefore make special efforts to follow the principle of accuracy.

301 Former Recital 41, Preamble to Directive 95/46/EC.

3.5. The storage limitation principle

Key points

- The principle of storage limitation means that personal data must be deleted or anonymised as soon as they are no longer needed for the purposes for which they were collected.

Article 5 (1) (e) of the GDPR and, likewise, Article 5 (4) (e) of Modernised Convention 108 require personal data to be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data" are processed. The data must therefore be erased or anonymised when those purposes have been served. To this end, "time limits should be established by the controller for erasure or for a periodic review" to make sure that the data are kept for no longer than is necessary.[302]

In *S. and Marper*, the ECtHR concluded that the core principles of the relevant instruments of the Council of Europe, and the law and practice of the other Contracting Parties, required data retention to be proportionate in relation to the purpose of collection and limited in time, particularly in the police sector.[303]

> Example: In *S. and Marper*,[304] the ECtHR ruled that indefinite retention of the fingerprints, cell samples and DNA profiles of the two applicants was disproportionate and unnecessary in a democratic society, considering that the criminal proceedings against both applicants had been terminated by an acquittal and a discontinuance, respectively.

The time limitation for storing personal data only applies to data kept in a form which permits identification of data subjects. Lawful storage of data which are no longer needed could, therefore, be achieved by anonymising data.

Archiving data for public interest, scientific or historical purposes, or for statistical use, may be stored for longer periods, providing such data will be used solely for

302 General Data Protection Regulation, Recital 39.

303 ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008; see also, for example: ECtHR, *M.M. v. the United Kingdom*, No. 24029/07, 13 November 2012.

304 ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008.

the above purposes.[305] Appropriate technical and organisational measures must be implemented for the ongoing storage and use of personal data to safeguard the rights and freedoms of the data subject.

Modernised Convention 108 also permits exceptions to the principle of storage limitation, on the condition that they are provided by law, respect the essence of fundamental rights and freedoms, and are necessary and proportionate for pursuing a limited number of legitimate aims.[306] These include, among others, protecting national security, investigating and prosecuting criminal offences, carrying out criminal penalties, protecting the data subject and protecting the rights and fundamental freedoms of others.

Example: In the *Digital Rights Ireland* case,[307] the CJEU reviewed the validity of the Data Retention Directive, which aimed to harmonise national provisions on the retention of personal data generated or processed by publicly available electronic communications services or networks to fight serious crime, such as organised crime and terrorism. The Data Retention Directive imposed a data retention period of "at least six months, without any distinction being made between the categories of data set out in Article 5 of that Directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned".[308] The CJEU also raised the issue of the absence of objective criteria in the Data Retention Directive, on the basis of which the exact period of data retention – which could vary from a minimum of six months to a maximum of 24 months – must be determined to ensure such a period is limited to what is strictly necessary.[309]

305 General Data Protection Regulation, Art. 5 (1) (e); Modernised Convention 108, Art. 5 (4) (b) and 11 (2).

306 Modernised Convention 108, Art. 11.1; Explanatory Report of Modernised Convention 108, paras. 91–98.

307 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [GC], 8 April 2014.

308 *Ibid.*, para. 63.

309 *Ibid.*, para. 64.

3.6. The data security principle

Key points

- The security and confidentiality of personal data are key to preventing adverse effects for the data subject.
- Security measures can be of a technical and/or organisational nature.
- Pseudonymisation is a process that can protect personal data.
- The appropriateness of security measures must be determined on a case-by-case basis and reviewed regularly.

The principle of data security requires that appropriate technical or organisational measures are implemented when processing personal data to protect the data against accidental, unauthorised or unlawful access, use, modification, disclosure, loss, destruction or damage. [310] The GDPR states that the controller and the processor should take into account "the state of the art, the costs of implementation and the nature, scope, context and purpose of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons" when implementing such measures.[311] Depending on the specific circumstances of each case, appropriate technical and organisational measures could include, for example, pseudonymising and encrypting personal data and/or regularly testing and evaluating the effectiveness of the measures to ensure the data processing is secure.[312]

As explained in Section 2.1.1, pseudonymising data means replacing the attributes in personal data – which make it possible to identify the data subject – with a pseudonym, and keeping those attributes separate, under technical or organisational measures. The process of pseudonymisation must not be confused with the process of anonymisation, where all links to identifying the person are broken.

Example: The sentence "Charles Spencer, born 3 April 1967, is the father of a family of four children, two boys and two girls" can, for instance, be pseudonymised as follows:

310 General Data Protection Regulation, Recital 39 and Art. 5 (1) (f); Modernised Convention 108, Art. 7.

311 General Data Protection Regulation, Art. 32 (1).

312 *Ibid.*

"C.S. 1967 is the father of a family of four children, two boys and two girls"; or

"324 is the father of a family of four children, two boys and two girls"; or

"YESz320I is the father of a family of four children, two boys and two girls".

Users who access pseudonymised data will usually have no ability to identify "Charles Spencer, born 3 April 1967" from "324" or "YESz3201". Such data are, therefore, more likely to be safe from misuse.

The first example is, however, less safe. If the sentence "C.S. 1967 is father of a family of four children, two boys and two girls" is used within the small village where Charles Spencer lives, Mr Spencer may be easily recognisable. The pseudonymisation method can affect the effectiveness of data protection.

Personal data with encrypted or separately kept attributes are used in many contexts as a means of keeping personal identities secret. This is particularly useful where data controllers need to ensure that they are dealing with the same data subjects but do not require, or ought not to have, the data subjects' real identities. This is the case, for example, where a researcher studies the course of a disease with patients, whose identity is known only to the hospital where they are treated and from which the researcher obtains the pseudonymised case histories. Pseudonymisation is therefore a strong link in the armoury of privacy-enhancing technology. It can function as an important element when implementing privacy by design. This means having data protection built into the fabric of data processing systems.

Article 25 of the GDPR, which addresses data protection by design, explicitly refers to pseudonymisation as an example of an appropriate technical and organisational measure that controllers should implement to accommodate the data protection principles and integrate the necessary safeguards. In doing so, controllers will meet the requirements of the regulation and will protect the rights of data subjects when processing their personal data.

Adherence to an approved code of conduct or an approved certification mechanism can help to demonstrate compliance with the security of processing requirement.[313] In its Opinion on the Data protection implications of the processing of Passenger Name Records, the Council of Europe provides other examples of appropriate

313 *Ibid.*, Art. 32 (3).

security measures for the protection of personal data in passenger name record systems. These include holding data in a secure physical environment, limiting access control via layered logins and protecting the communication of data with strong cryptography.[314]

Example: Social networking sites and email providers make it possible for users to add an extra layer of data security to the services they provide through the introduction of two-tier authentication. In addition to entering a personal password, users must complete a second sign-in to enter their personal account. The latter could be, for instance, the entry of a security code sent to the mobile number connected to the personal account. In this way, two-step verification provides better protection of personal information against unauthorised access to personal accounts via hacking.

The Explanatory Report of Modernised Convention 108 provides additional examples of appropriate safeguards, such as the implementation of a professional secrecy obligation, or the adoption of qualified technical security measures such as data encryption.[315] When putting specific security measures in place, the controller – or, where applicable, the processor – should take into account several elements, such as the nature and volume of the personal data processed, potential adverse consequences for data subjects, and the need for restricted data access.[316] The current state of the art of data security methods and techniques for data processing must be considered when implementing appropriate security measures. The cost of such measures must be proportionate to the seriousness and probability of potential risks. A regular review of the security measures is required so that they may be updated as necessary.[317]

In cases where a personal data breach takes place, both Modernised Convention 108 and the GDPR require the controller to notify the competent supervisory authority of the breach with risks for rights and freedoms of individuals without undue delay.[318] A similar communication obligation to the data subject exists when the personal

314 Council of Europe, Committee of Convention 108, *Opinion on the Data protection implications of the processing of Passenger Name Records*, T-PD(2016)18rev, 19 August 2016, p. 9.

315 Explanatory Report of Modernised Convention 108, para. 56.

316 *Ibid.*, para. 62.

317 *Ibid.*, para. 63.

318 Modernised Convention 108, Art. 7 (2); General Data Protection Regulation, Art. 33 (1).

data breach is likely to result in a high risk to his or her rights and freedoms.[319] Communication of such breaches to the data subjects must be in clear and plain language.[320] If the processor becomes aware of a personal data breach, the controller must be notified immediately.[321] In certain situations, exceptions to the notification obligation may apply. For instance, the controller is not required to notify the supervisory authority when "the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons".[322] Nor is it necessary to notify the data subject when implemented security measures render the data unintelligible for non-authorised persons or when subsequent measures ensure that the high risk is no longer likely to materialise.[323] If communication of a personal breach to the data subjects would involve disproportionate effort on behalf of the controller, a public communication or similar measure can ensure that "the data subjects are informed in an equally effective manner".[324]

3.7. The accountability principle

Key points

- Accountability requires controllers and processors to actively and continuously implement measures to promote and safeguard data protection in their processing activities.
- Controllers and processors are responsible for compliance of their processing operations with data protection law and their respective obligations.
- Controllers must be able to demonstrate compliance with data protection provisions to data subjects, the general public and supervisory authorities at any time. Processors must also comply with some obligations strictly linked to accountability (such as keeping a record of processing operations and appointing a Data Protection Officer).

The GDPR and Modernised Convention 108 set out that the controller is responsible for, and must be able to demonstrate compliance with, the personal data processing principles described in this chapter.[325] To this end, the controller must implement

319 Modernised Convention 108, Art. 7 (2); General Data Protection Regulation, Art. 34 (1).

320 General Data Protection Regulation, Art. 34 (2).

321 *Ibid.*, Art. 33 (1).

322 *Ibid.*, Art. 32 (1).

323 *Ibid.*, Art. 34 (3) (a) and (b).

324 *Ibid.*, Art. 34 (3) (c).

325 *Ibid.*, Art. 5 (2); Modernised Convention 108, Art. 10 (1).

appropriate technical and organisational measures.[326] Even though the accountability principle in Article 5 (2) of the GDPR is only directed towards controllers, processors are also expected to be accountable, given that they have to comply with several obligations and that they are closely connected to accountability.

EU and CoE data protection laws also determine that the controller is responsible for, and should be able to ensure, compliance with the data protection principles discussed in Sections 3.1 to 3.6.[327] The Article 29 Working Party points out that "the type of procedures and mechanisms would vary according to the risks represented by the processing and the nature of the data".[328]

Controllers can facilitate compliance with this requirement in various ways, which include:

- recording processing activities and making them available to the supervisory authority upon request;[329]
- in certain situations, designating a data protection officer who is involved in all issues relating to personal data protection;[330]
- undertaking data protection impact assessments for types of processing likely to result in a high risk to the rights and freedoms of natural persons;[331]
- ensuring data protection by design and by default;[332]
- implementing modalities and procedures for the exercise of the rights of the data subjects;[333]
- adhering to approved codes of conduct or certification mechanisms.[334]

326 General Data Protection Regulation, Art. 24.

327 *Ibid.*, Art. 5 (2); Modernised Convention 108, Art. 10 (1).

328 Article 29 Working Party, *Opinion 3/2010 on the principle of accountability*, WP 173, Brussels, 13 July 2010, para. 12.

329 General Data Protection Regulation, Art. 30.

330 *Ibid.*, Art. 37–39.

331 *Ibid.*, Art. 35; Modernised Convention 108, Art. 10 (2).

332 General Data Protection Regulation, Art. 25; Modernised Convention 108, Art. 10 (2) and (3).

333 *Ibid.*, Art. 12 and Art. 24.

334 *Ibid.*, Art. 40 and Art. 42.

While the principle of accountability in Article 5 (2) of the GDPR is not specifically directed to processors, there are provisions linked to accountability that also contain obligations for them, such as keeping a record of processing activities and appointing a Data Protection Officer for any processing activities that require one.[335] Processors must also ensure that all measures necessary for ensuring the security of the data have been implemented.[336] The legally binding contract between the controller and the processor must set out that the processor shall assist the controller in some of the compliance requirements, such as when carrying out a data protection impact assessment or notifying the controller of any personal data breach as soon as they become aware of it.[337]

The Organisation for Economic Co-operation and Development (OECD) adopted privacy guidelines in 2013 that highlighted that controllers have an important role in making data protection work in practice. The guidelines comprise an accountability principle to the effect that "a data controller should be accountable for complying with measures which give effect to the [material] principles stated above."[338]

Example: A legislative example for stressing the principle of accountability is the 2009 amendment[339] to the e-Privacy Directive 2002/58/EC. According to Article 4 in its amended form, the directive imposes an obligation to "ensure the implementation of a security policy with respect to the processing of personal data". Thus, as far as the security provisions of that directive are concerned, the legislator decided that it was necessary to introduce an explicit requirement to have, and implement, a security policy.

335 *Ibid.*, Art. 5 (2), 30 and 37.

336 *Ibid.*, Art. 28 (3) c.

337 *Ibid.*, Art. 28 (3) d.

338 OECD (2013), *Guidelines on governing the Protection of Privacy and transborder flows of personal data*, Art. 14.

339 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services; Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ 2009 L 337, p. 11.

According to the Article 29 Working Party's opinion,[340] the essence of accountability is the controller's obligation to:

- put in place measures which would – under normal circumstances – guarantee that data protection rules are adhered to in the context of processing operations; and

- have documentation ready which demonstrates to data subjects and to supervisory authorities the measures that have been taken to achieve compliance with the data protection rules.

The principle of accountability thus requires controllers to actively demonstrate compliance and not merely wait for data subjects or supervisory authorities to point out shortcomings.

340 Article 29 Working Party, *Opinion 3/2010 on the principle of accountability*, WP 173, Brussels, 13 July 2010.

4

Rules of European data protection law

EU	Issues covered	CoE
Rules on lawful processing of data		
General Data Protection Regulation, Article 6 (1) (a) CJEU, C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, 2011 CJEU, C-536/15, *Tele2 (Netherlands) BV and Others v. Autoriteit Consument en Markt (AMC)*, 2017	**Consent**	Profiling Recommendation, Articles 3.4 (b) and 3.6 Modernised Convention 108, Article 5 (2)
General Data Protection Regulation, Article 6 (1) (b)	**(Pre-)contractual relationship**	Profiling Recommendation, Article 3.4 (b)
General Data Protection Regulation, Article 6 (1) (c)	**Legal duties of the controller**	Profiling Recommendation, Article 3.4 (a)
General Data Protection Regulation, Article 6 (1) (d)	**Vital interests of the data subject**	Profiling Recommendation, Article 3.4 (b)
General Data Protection Regulation, Article 6 (1) (e) CJEU, C-524/06, *Huber v. Bundesrepublik Deutschland* [GC], 2008	**Public interest and exercise of official authority**	Profiling Recommendation, Article 3.4 (b)

EU	Issues covered	CoE
General Data Protection Regulation, Article 6 (1) (f) CJEU, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme'*, 2017 CJEU, Joined cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 2011	**Legitimate interests of others**	Profiling Recommendation, Article 3.4 (b) ECtHR, *Y v. Turkey*, No. 648/10, 2015
General Data Protection Regulation, Article 6 (4)	**Exception to purpose limitation: further processing for other purposes**	Modernised Convention 108, Article 5 (4) (b)
Rules on lawful processing of sensitive data		
General Data Protection Regulation, Article 9 (1)	**General prohibition to process**	Modernised Convention 108, Article 6
General Data Protection Regulation, Article 9 (2)	**Exemptions from the general prohibition**	Modernised Convention 108, Article 6
Rules on secure processing		
General Data Protection Regulation, Article 32	**Obligation to ensure secure processing**	Modernised Convention 108, Article 7 (1) ECtHR, *I v. Finland*, No. 20511/03, 2008
General Data Protection Regulation, Article 28 and 32 (1) (b)	**Obligation to confidentiality**	Modernised Convention 108, Article 7 (1)
General Data Protection Regulation, Article 34 Directive on privacy and electronic communications, Article 4 (2)	**Data breach notifications**	Modernised Convention 108, Article 7 (2)
Rules on accountability and promoting compliance		
General Data Protection Regulation, Articles 12, 13 and 14	**Transparency in general**	Modernised Convention 108, Article 8
General Data Protection Regulation, Articles 37, 38 and 39	**Data Protection Officers**	Modernised Convention 108, Article 10 (1)

EU	Issues covered	CoE
General Data Protection Regulation, Article 30	Records of processing activities	
General Data Protection Regulation, Articles 35 and 36	Impact assessment and prior consultation	Modernised Convention 108, Article 10 (2)
General Data Protection Regulation, Articles 33 and 34	Data breach notifications	Modernised Convention 108, Article 7 (2)
General Data Protection Regulation, Articles 40 and 41	Codes of conduct	
General Data Protection Regulation, Articles 42 and 43	Certification	
Data protection by design and by default		
General Data Protection Regulation, Article 25 (1) (a)	Data protection by design	Modernised Convention 108, Article 10 (2)
General Data Protection Regulation, Article 25 (1) (b)	Data protection by default	Modernised Convention 108, Article 10 (3)

Principles are necessarily of a general nature. Their application to concrete situations leaves a certain margin of interpretation and choice of means. Under **CoE law**, it is left to the parties to Modernised Convention 108 to clarify this margin of interpretation in their domestic law. The situation in **EU law** is different: for the establishment of data protection in the internal market, it was deemed necessary to have more detailed rules at the EU level to harmonise the level of data protection of the national laws of the Member States. The General Data Protection Regulation establishes a layer of detailed rules, under the principles set out in its Article 5, which are directly applicable in the national legal order. The following remarks on detailed data protection rules at the European level therefore predominantly deal with EU law.

4.1. Rules on lawful processing

Key points

- Personal data may be lawfully processed if they meet one of the following criteria:
  - the processing is based on the consent of the data subject;
  - a contractual relationship requires the processing of personal data;

  - the processing is necessary for compliance with a legal obligation of the controller;
  - vital interests of data subjects or of another person require the processing of their data;
  - the processing is needed for the performance of a task in the public interest;
  - legitimate interests of controllers or third parties are the reason for processing, but only as long as they are not overridden by the interests or the fundamental rights of the data subjects.
- Lawful processing of sensitive personal data is subject to a special, stricter regime.

4.1.1. Lawful grounds for processing data

Chapter II of the General Data Protection Regulation, entitled 'Principles', provides that all personal data processing must comply, firstly, with the principles relating to data quality set out in Article 5 of the GDPR. One of the principles is that personal data should be "processed lawfully, fairly and in a transparent way". Secondly, for data to be processed lawfully, the processing must comply with one of the lawful grounds for making data processing legitimate, listed in Article 6[341] for non-sensitive personal data, and in Article 9 for special categories of data (or sensitive data). Similarly, Chapter II of Modernised Convention 108 which sets out the "basic principles for the protection of personal data", establishes that to be lawful, data processing shall be "proportionate in relation to the legitimate purpose pursued".

Irrespective of the lawful ground for processing that a controller relies on to initiate a personal data processing operation, the controller will also have to apply the safeguards provided for in the general data protection law regime.

Consent

Under CoE law, consent is mentioned in Article 5 (2) of Modernised Convention 108. It is also referred to in ECtHR case law and several CoE recommendations.[342] **Under**

341 CJEU, Joined cases C-465/00, C-138/01 and C-139/01, *Rechnungshof v. Österreichischer Rundfunk and Others* and *Christa Neukomm and Jospeh Lauermann v. Österreichischer Rundfunk*, 20 May 2003, para. 65; CJEU, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland* [GC], 16 December 2008, para. 48; CJEU, Joined cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 November 2011, para. 26.

342 See for example, Council of Europe, Committee of Ministers (2010), Recommendation CM/Rec(2010)13 of the Committee of Ministers to the Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 23 November 2010, Art. 3.4 (b).

EU law, consent as a basis for lawful data processing is firmly established in Article 6 of the GDPR and is also explicitly referred to in Article 8 of the Charter. The characteristics of valid consent are explained in the definition of consent in Article 4, while the conditions for obtaining valid consent are detailed in Article 7 and the special rules for child's consent in relation to information society services are established in Article 8 of the GDPR.

As explained in Section 2.4, consent must be freely given, informed, specific, and unambiguous. Consent must be a statement or clear affirmative action signifying agreement to the processing, and the person has the right to withdraw their consent at any time. Controllers have the duty to keep a verifiable record of the consent.

Free consent

Within the **CoE** framework of Modernised Convention 108, consent of the data subject must "represent the free expression of an intentional choice".[343] The existence of free consent is only valid "if the data subject is able to exercise a real choice and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent".[344] In this regard, **EU law** stipulates that consent is not considered freely given "if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment".[345] The GDPR stresses that "(w)hen assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract".[346] The Explanatory Report of Modernised Convention 108 states that "[n]o undue influence or pressure (which can be of an economic or other nature) whether direct or indirect, may be exercised on the data subject and consent should not be regarded as freely given where the data subject has no genuine choice or is unable to refuse or withdraw consent without prejudice".[347]

343 Explanatory Report of Modernised Convention 108, para. 42.

344 See also Article 29 Working Party (2011), *Opinion 15/2011 on the notion of consent*, WP 187, Brussels, 13 July 2011, p. 12.

345 General Data Protection Regulation, Recital 42.

346 *Ibid*., Art. 7 (4).

347 Explanatory Report of Modernised Convention 108, para. 42.

Example: Some municipalities in State A decided to develop residence cards with an embedded chip. It is not compulsory for residents to acquire those electronic cards. However, residents who do not possess the card do not have access to a series of important administrative services, such as the ability to pay municipal taxes online, to submit complaints electronically benefiting from a three-day deadline for the authority to respond, and even to skip queues, buy reduced tickets when visiting the municipal concert hall and use the scanners in the entrance.

The municipalities' processing of personal data in this example cannot be based on consent. Since there is at least an indirect pressure for residents to obtain the electronic card and agree to the processing, consent is not given freely. The municipalities' development of an electronic cards system should thus be based on another legitimate ground justifying the processing. For instance, they could invoke that processing is necessary for the performance of a task carried out in the public interest, which is a lawful basis for processing pursuant to Article 6 (1) (e) of the GDPR.[348]

Free consent could also be in doubt in situations of subordination, where there is a significant economic or other imbalance between the controller securing consent and the data subject providing consent.[349] A typical example of such imbalances and subordination is an employer's processing of personal data, within the context of an employment relationship. According to the Article 29 Working Party, "[e]mployees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer."[350]

348 Article 29 Working Party (2011), *Opinion 15/2011 on the definition of consent*, WP187, Brussels, 13 July 2011, p. 16. Further examples of cases where data processing cannot be based on consent, but requires a different legal ground for legitimising the processing, can be found in pp. 14 and 17 of the opinion.

349 See also Article 29 Working Party (2001), *Opinion 8/2001 on the processing of personal data in the employment context*, WP 48, Brussels, 13 September 2001; Article 29 Working Party (2005), Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995, WP 114, Brussels, 25 November 2005; Article 29 Working Party (2017), *Opinion 2/2017 on data processing at work*, WP 249, Brussels, 8 June 2017.

350 Article 29 Working Party, *Opinion 2/2017 on data processing at work*, WP 249, Brussels, 8 June 2017.

Example: A large company plans to create a directory containing the names of all employees, their function in the company and their business addresses, solely to improve internal company communications. The head of personnel proposes adding a photo of each employee to the directory to make it easier to recognise colleagues at meetings. Employees' representatives demand that this should be done only if the individual employee consents.

In such a situation, an employee's consent should be acknowledged as the legal basis for processing the photos in the directory because it is credible that the employee will not face any consequences at all, whether he or she decides to agree or not to have his or her photo published in the directory.

Example: Company A is planning a meeting, between three of its employees and the directors of Company B, to discuss potential future cooperation on a project. The meeting will take place at the premises of Company B, who requires Company A to email them the names, CVs and photos of the participants to the meeting. Company B argues that it needs the names and photos of the participants to allow security staff at the building's entrance to check that they are the right persons, while the CVs will enable the directors to better prepare for the meeting. In this case, Company A's transmission of its employees' personal data cannot be based on consent. Consent could not be considered as 'freely given', as it is possible that the employees may face negative consequences if they reject the offer (for example, they might be replaced by another colleague not only in attending the meeting, but also in liaising with Company B and contributing to the project in general). Therefore, the processing must be based on another lawful ground for processing.

This does not mean, however, that consent can never be valid in circumstances where not consenting would have some negative consequences. For instance, if not consenting to having a supermarket's customer card only results in not receiving a small reduction in the price of certain goods, consent could be a valid legal basis for processing the personal data of those customers who consented to having such a card. There is no subordination between company and customer and the consequences of not consenting are not serious enough to prevent the data subject's free choice (provided that the price reduction is small enough not to affect their free choice).

However, where goods or services can only be obtained if certain personal data are disclosed to the controller or further on to third parties, the data subject's consent to disclose their data, which are not necessary for the contract, cannot be considered

a free decision and is, therefore, not valid under data protection law.[351] The GDPR is rather strict in forbidding the bundling of consent with the provision of goods and services.[352]

Example: Passengers' agreement to an airline that transmits so-called passenger name records (i.e. data on their identities, eating habits or health problems) to the immigration authorities of a specific foreign country cannot be considered valid consent under data protection law, as the travelling passengers have no choice if they want to visit this country. If such data are to be transmitted lawfully, some legal basis other than consent is required, most likely a specific law.

Informed consent

The data subject must have sufficient information before exercising his or her choice. Informed consent will usually comprise a precise and easily understandable description of the subject matter requiring consent. As the Article 29 Working Party explains, consent must be based upon an appreciation and understanding of the facts and implications of the data subject's action to consent to the processing. Therefore, "[t]he individual concerned must be given, in a clear and understandable manner, accurate and full information of all relevant issues [...] such as the nature of the data processed, purposes of the processing, the recipients of possible and the rights of the data subject."[353] For consent to be informed, individuals must also be aware of the consequences of not consenting to processing.

In view of the importance of informed consent, the GDPR and the Explanatory Report of Modernised Convention 108 sought to clarify the notion. The recitals of the GDPR stipulate that informed consent means that "the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data" processed are intended.[354]

In the exceptional case of consent used as a derogation to ensure a lawful ground for an international data transfer, the controller must inform the data subject of the

351 General Data Protection Regulation, Art. 7 (4).

352 *Ibid.*

353 Article 29 Working Party (2007), Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131, Brussels, 15 February 2007.

354 General Data Protection Regulation, Recital 42.

possible risks of such a transfer, due to the absence of an adequacy decision and appropriate safeguards, for that consent to be considered valid.[355]

The Explanatory Report of Modernised Convention 108 specifies that information must be given on the implications of the data subject's decision, namely "what the fact of consenting entails and the extent to which consent is given".[356]

The quality of the information is important. Quality of information means that the information's language should be adapted to its foreseeable recipients. Information must be given without jargon, in a clear and plain language that a regular user should be able to understand.[357] Information must also be easily available to the data subject and can be provided orally or in writing. Accessibility and visibility of the information are important elements: the information must be clearly visible and prominent. In an online environment, layered information notices may be a good solution, as these allow data subjects to choose whether to access concise or more extensive versions of information.

Specific consent

For consent to be valid, it must also be specific to the processing purpose, which must be described clearly, and in unambiguous terms. This goes hand-in-hand with the quality of information given about the purpose of the consent. In this context, the reasonable expectations of an average data subject will be relevant. The data subject must be asked again for consent if processing operations are to be added or changed in a way which could not have reasonably been foreseen when the initial consent was given and thus lead to a change of purpose. When the processing has multiple purposes, consent should be given for all of them.[358]

Examples: In *Deutsche Telekom AG*,[359] the CJEU considered whether a telecom provider that had to pass on personal data of subscribers to be published in

355 *Ibid.*, Art. 49 (1) (a).

356 Explanatory Report of Modernised Convention 108, para. 42.

357 Article 29 Working Party (2011), *Opinion 15/2011 on the definition of consent*, WP187, Brussels, 13 July 2011, p. 19.

358 General Data Protection Regulation, Recital 32.

359 CJEU, C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, 5 May 2011. See especially paras. 53 and 54.

directories needed renewed consent from the data subjects,[360] as the data's recipients were not originally named when consent was given.

The CJEU held that, under Article 12 of the Directive on privacy and electronic communications, renewed consent was not necessary before passing on the data. Since the data subjects only had the option to consent to the purpose of the processing – which was the publication of their data – they could not choose between different directories in which these data might be published.

As the CJEU underlined, "it follows from a contextual and systematic interpretation of Article 12 of the Directive on privacy and electronic communications that the consent under Article 12 (2) relates to the purpose of the publication of personal data in a public directory and not to the identity of any particular directory provider."[361] In addition, "it is the publication itself of the personal data in a public directory with a specific purpose which may turn out to be detrimental for a subscriber",[362] rather than being a matter of the identity of the publisher.

Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV v. Autoriteit Consument en Markt (AMC)[363] concerned Belgian company's request that directory enquiry services and directories to companies that assign telephone numbers in the Netherlands provide it with access to data related to their subscribers. The Belgian company relied on an obligation under the Universal Services Directive.[364] This requires companies that assign telephone numbers to make the numbers available for directories that request them, if subscribers consented to have their numbers published. The Dutch companies refused to do so, stating that they were not required to provide the data in question to an undertaking established in another Member State. They argued that users gave their consent for publication of their numbers on the

360 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ 2002 L 201 (Directive on privacy and electronic communications).

361 CJEU, C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, 5 May 2011; para. 61.

362 *Ibid.*, para. 62.

363 CJEU, C-536/15, *Tele2 (Netherlands) BV and Others v. Autoriteit Consument en Markt (AMC)*, 15 March 2017.

364 Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), OJ 2002 L 108, p. 51, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (Universal Services Directive), OJ 2009 L 337, p. 11.

understanding that they would be published in a Dutch directory. The CJEU held that the Universal Services Directive covers all requests by directory services undertakings, irrespective of the Member State in which they are established. The CJEU also held that the passing of the same data to another undertaking intending to publish a public directory without obtaining renewed consent from the subscribers, is not capable of substantively impairing the right to the protection of personal data.[365] Consequently, it is not necessary for the undertaking assigning telephone numbers to its subscribers to differentiate in the request for consent addressed to the subscriber according to the Member State to which the data concerning him could be sent.[366]

Unambiguous consent

All consent must be given in an unambiguous way.[367] This means that there should be no reasonable doubt that the data subject wanted to express his or her agreement to allow the processing of his or her data. For instance, inactivity from a data subject does not indicate unambiguous consent.

This would be the case for controller's obtaining consent with statements in their privacy policies such as "by using our service, you consent to the processing of your personal data". In that case, controllers might have to ensure that users manually and individually consent to such policies.

If consent is given in a written form which is part of a contract, consent for processing personal data must be individualised and in any case "safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given."[368]

Consent requirements for children

The GDPR provides specific protection for children in the context of providing information society services, because "they may be less aware of the risks,

365 CJEU, C-536/15, *Tele2 (Netherlands) BV and Others v. Autoriteit Consument en Markt (AMC)*, 15 March 2017, para. 36.

366 *Ibid*., paras. 40-41.

367 General Data Protection Regulation, Art. 4 (11).

368 *Ibid*., Recital 42.

consequences and safeguards concerned and their rights in relation to the processing of personal data".[369] Therefore, under **EU law**, when providers of information society services process personal data of children under the age of 16 years on the basis of consent, such processing will be lawful "only if, and to the extent that, consent is given or authorised by the holder of parental responsibility over the child".[370] Member States may provide for a lower age in national law, though not lower than 13 years.[371] Consent by the holder of parental responsibility is not necessary "in the context of preventive or counselling services offered directly to a child."[372] Information and communication where processing is addressed to a child should be in clear and plain language easily understandable by the child.[373]

The right to withdraw consent at any time

The GDPR includes a general right to withdraw consent at any time.[374] The data subject must be informed of such a right prior to giving consent and he or she may exercise this right at his or her discretion. There should be no requirement to give reasons for withdrawal and no risk of negative consequences over and above the termination of any benefits which may have derived from the previously agreed data use. Withdrawing consent should be as easy as giving it.[375] There can be no free consent if the data subject is unable to withdraw his or her consent without detriment or if withdrawal is not as easy as giving consent had been.[376]

Example: A customer agrees to receiving promotional mail to an address he or she provides to a data controller. Should the customer withdraw consent, the controller must immediately stop sending promotional mail. No punitive consequences such as fees should be imposed. The withdrawal however is exercised for the future, and does not have retroactive effect. The period

369 *Ibid.*, Recital 38.

370 *Ibid.* Art. 8 (1) first indent. The notion of information society services is defined in Art. 4 (25) of the General Data Protection Regulation.

371 General Data Protection Regulation, Art. 8 (1) second indent.

372 *Ibid.*, Recital 38.

373 *Ibid.*, Recital 58. See also Modernised Convention 108, Art. 15 (2) (e). Explanatory Report of Modernised Convention 108, paras. 68 and 125.

374 General Data Protection Regulation, Art. 7 (3). Explanatory Report of Modernised Convention 108, para. 45.

375 General Data Protection Regulation, Art. 7 (3).

376 General Data Protection Regulation, Recital 42; Explanatory Report of Modernised Convention 108, para. 42.

in which the customer's personal data was processed lawfully – because of the customer's consent – had been legitimate. The withdrawal prevents any further processing of these data, unless such processing is in accordance with the right to erasure.[377]

Necessity for the performance of a contract

Under EU law, Article 6 (1) (b) of the GDPR provides another basis for legitimate processing, namely if it is "necessary for the performance of a contract to which the data subject is party". This provision also covers pre-contractual relationships. For instance, in cases where a party intends to enter into a contract, but has not yet done so, possibly because some checks remain to be completed. If one party needs to process data for this purpose, such processing is legitimate as long as it is "necessary in order to take steps at the request of the data subject prior to entering into a contract".[378]

The notion of data processing as a "legitimate basis laid down by law" in Article 5 (2) of Modernised Convention 108 also encompasses "data processing for the fulfilment of a contract (or pre-contractual measures at the request of the data subject) to which the data subject is party".[379]

Legal duties of the controller

EU law sets out another ground for making data processing legitimate, namely if "it is necessary for compliance with a legal obligation to which the controller is subject" (Article 6(1) (c) of the GDPR). This provision refers to controllers acting in both the private and public sector; the legal obligations of public sector data controllers can also fall under Article 6 (1) (e) of the GDPR. There are many examples of situations where the law obliges private sector controllers to process data about concrete data subjects. For instance, employers must process data about their employees for social security and taxation reasons, and businesses must process data about their customers for tax purposes.

377 General Data Protection Regulation, Art. 17 (1) (b).

378 *Ibid*., Art. 6 (1) (b).

379 Explanatory Report of Modernised Convention 108, para. 46; Council of Europe, Committee of Ministers (2010), Recommendation CM/Rec(2010)13 of the Committee of Ministers to the Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 23 November 2010, Art. 3.4 (b).

The legal obligation can originate in Union or Member State law, which could be the basis for one or several processing operations. It should be for the law to determine the purpose of processing, establish specifications to determine the controller, the type of personal data subject to processing, the data subjects concerned, the entities to which the data can be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing.[380] Any such law that is the basis for personal data processing must comply both with Articles 7 and 8 of the Charter and Article 8 of the ECHR.

The controller's legal obligations also serve as a basis for legitimate data processing **under CoE law.**[381] As previously pointed out, the legal obligations of a private sector controller are just one specific case of the legitimate interests of others, as mentioned in Article 8 (2) of the ECHR. The example on employers processing data about their employees is, therefore, also relevant for CoE law.

Vital interests of the data subject or those of another natural person

Under EU law, Article 6 (1) (d) of the GDPR provides that personal data processing is lawful if it "is necessary in order to protect the vital interests of the data subject or of another natural person". This legitimate ground may only be invoked for processing personal data based on the vital interests of another natural person, if such processing "cannot be manifestly based on another legal basis".[382] Sometimes a type of processing may be based on the grounds of both public interest and the vital interests of the data subject or that of another person. This is the case, for example, when monitoring epidemics and their development, or where there is a humanitarian emergency.

Under CoE law, the vital interests of the data subject are not mentioned in Article 8 of the ECHR. However, the vital interests of the data subject are considered to be implied in the notion of 'legitimate basis' of Article 5 (2) of Modernised Convention 108, which deals with the legitimacy of personal data processing.[383]

380 General Data Protection Regulation, Recital 45.

381 Council of Europe, Committee of Ministers (2010), Recommendation CM/Rec (2010) 13 of the Committee of Ministers to the Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 23 November 2010, Art. 3.4 (a).

382 General Data Protection Regulation, Recital 46.

383 Explanatory Report of Modernised Convention 108, para. 46.

Public interest and exercise of official authority

Given the many possible ways of organising public affairs, Article 6 (1) (e) of the GDPR provides that personal data may lawfully be processed if it "is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller [...]".[384]

Example: In *Huber v. Bundesrepublik Deutschland*,[385] Mr Huber, an Austrian national residing in Germany, asked the Federal Office for Migration and Refugees to delete data on him in the Central Register of Foreign Nationals ('the AZR'). This register, which contains personal data on non-German EU nationals who are resident in Germany for more than three months, is used for statistical purposes and by law enforcement and judicial authorities when investigating and prosecuting criminal activities or those which threaten public security. The referring court asked whether the processing of personal data which is undertaken in a register such as the Central Register of Foreign Nationals – to which other public authorities also have access – is compatible with EU law given that no such register exists for German nationals.

The CJEU held that, according to Article 7 (e) of Directive 95/46,[386] personal data may lawfully be processed if it is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority.

According to the CJEU, "having regard to the objective of ensuring an equivalent level of protection in all Member States, the concept of necessity laid down by Article 7 (e) of Directive 95/46[387] [...] cannot have a meaning which varies between Member States. It, therefore, follows that what is at issue is a concept which has its own independent meaning in Community law and which must be interpreted in a manner which fully reflects the objective of that directive, as laid down in Article 1 (1) thereof".[388]

384 See General Data Protection Regulation, Recital 45.

385 CJEU, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland* [GC], 16 December 2008.

386 Former Data Protection Directive, Art. 7 (e), now General Data Protection Regulation, Art. 6 (1) (e).

387 *Ibid*.

388 CJEU, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland* [GC], 16 December 2008, para. 52.

The CJEU noted that the right of free movement of a Union citizen in a Member State's territory of which he or she is not a national is not unconditional and may be subject to limitations and conditions imposed by the Treaty Establishing the European Community and by the measures adopted to give it effect. Thus, if it is, in principle, legitimate for a Member State to use a register such as the AZR to support the authorities responsible for applying the legislation relating to the right of residence, such a register must not contain any information other than what is necessary for that particular purpose. The CJEU concluded that such a system for processing personal data complies with EU law if it only contains the data necessary to apply that legislation and if its centralised nature makes the application of that legislation more effective. The national court must ascertain whether those conditions are satisfied in this particular case. If not, the storage and processing of personal data in a register such as the AZR for statistical purposes cannot, on any basis, be considered to be necessary within the meaning of by Article 7 (e) [389] of Directive 95/46.[390]

Lastly, as regards the question of the use of the data contained in the register for the purposes of fighting crime, the CJEU held that this objective "necessarily involves the prosecution of crimes and offences committed, irrespective of the nationality of their perpetrators". The register at issue does not contain personal data relating to nationals of the Member State concerned and this difference in treatment constitutes a discrimination prohibited by Article 18 of the TFEU. Consequently, the CJEU found that this provision "precludes the putting in place by a Member State, for the purpose of fighting crime, of a system for processing personal data specific to Union citizens who are not nationals of that Member State."[391]

The use of personal data by authorities acting in the public arena is also subject to Article 8 of the **ECHR** and is meant to be covered, where appropriate, by Article 5 (2) of Modernised Convention 108.[392]

389 Former Data Protection Directive, Art. 7 (e), now General Data Protection Regulation, Art. 6 (1) (e).

390 CJEU, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland* [GC], 16 December 2008, paras. 54, 58–59 and 66–68.

391 *Ibid.*, paras. 78 and 81.

392 Explanatory Report of Modernised Convention 108, paras. 46 and 47.

Legitimate interests pursued by the controller or by a third party

Under **EU law**, the data subject is not the only one with legitimate interests. Article 6 (1) (f) of the GDPR provides that personal data may lawfully be processed if it "is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties [except public authorities in the performance of their tasks] to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection [...]".[393]

The existence of a legitimate interest must be carefully assessed in each specific case.[394] If the legitimate interests of the controller are identified, then a balancing exercise must be conducted between those interests and the interests or fundamental rights and freedoms of the data subject.[395] The reasonable expectations of the data subject must be considered during such an assessment to ascertain whether the interests of the controller override the interests or fundamental rights of the data subject.[396] If the data subject's rights override the controller's legitimate interests, then the controller can take measures and implement safeguards to ensure that the impact on the data subject's rights is minimised (such as pseudonymising data), and invert the 'balance' before being able to lawfully rely on this legitimate basis for processing. In its Opinion on the notion of legitimate interests of the data controller, the Article 29 Working Party underlined the crucial role of accountability and transparency, and of the data subject's rights to object to the processing of their data, or to it being accessed, modified, deleted or transferred, when balancing the legitimate interests of the controller and the interests of the data subject's fundamental rights.[397]

In the GDPR recitals, some examples are given as to what constitutes a legitimate interest of the data controller concerned. For instance, the processing personal data is allowed without the data subject's consent when it is done for direct marketing

393 Compared to Directive 95/46, the General Data Protection Regulation provides more examples of cases that are considered to constitute a legitimate interest.

394 General Data Protection Regulation, Preamble, Recital 47.

395 Article 29 Working Party (2014), *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 4 April 2014.

396 *Ibid*.

397 *Ibid*.

purposes or when such processing is "strictly necessary for the purposes of preventing fraud".[398]

In its case law, the CJEU has expanded on the test to determine what constitutes a legitimate interest.

Example: The *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde* case[399] concerned damage to a Rīgas Transport Company trolleybus caused by a passenger suddenly opening a taxi door. Rīgas satiksme wanted to sue the passenger for damages. However, the police would only give the name of the passenger and refused to provide the passenger's ID number and address, arguing that the disclosure would be unlawful under national data protection laws.

The Latvian referring court asked the CJEU to deliver a preliminary ruling on whether EU data protection legislation imposes an obligation to disclose all the personal data necessary to launch civil proceedings against the person allegedly responsible for an administrative offence.[400]

The CJEU clarified that EU data protection law includes the possibility – not an obligation – of communicating data to a third party for the purposes of the legitimate interests pursued by that party.[401] The CJEU set out three cumulative conditions that must be fulfilled for personal data processing to be lawful on the 'legitimate interests' ground.[402] Firstly, the third party to whom the data are disclosed must pursue a legitimate interest. In this specific case, this means that requesting personal information to sue a person for causing property damage constitutes a legitimate interest of a third party. Secondly, the processing of personal data must be necessary for the purposes of the legitimate interests pursued. In this case, obtaining personal information such as the address and/or ID number is strictly necessary to identify that person. Thirdly, the fundamental rights and freedoms of the data subject must not take precedence over the controller's or third parties' legitimate

398 General Data Protection Regulation, Preamble, Recital 47.

399 CJEU, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme'*, 4 May 2017.

400 *Ibid.,* para. 23.

401 *Ibid.,* para. 26.

402 *Ibid.,* paras. 28–34.

interests. The balance of interests must be done on a case-by-case basis, taking into account elements such as the severity of the infringement of the data subject's rights or even the age of the data subject in certain circumstances. However, in this specific case the CJEU did not consider the refusal of disclosure to be justified simply because the data subject was a minor.

In the *ASNEF and FECEMD* judgment, the CJEU ruled explicitly on processing data based on the 'legitimate interests' lawful ground, which at that time was enshrined in Article 7 (f) of the Data Protection Directive.[403]

Example: In *ASNEF and FECEMD*,[404] the CJEU clarified that national law is not allowed to add conditions to those mentioned in Article 7 (f) of the Directive for lawful processing of data.[405] This referred to a situation where Spanish data protection law contained a provision whereby other private parties could claim a legitimate interest in processing personal data only if the information had already appeared in public sources.

The CJEU first noted that Directive 95/46[406] is intended to ensure that the level of protection of the rights and freedoms of individuals regarding the processing of personal data is equivalent in all Member States. Nor must the approximation of the national laws applicable in this area result in any decrease of the protection they afford. It must instead seek to ensure a high level of protection in the EU.[407] Consequently, the CJEU held that "it follows from the objective of ensuring an equivalent level of protection in all Member States that Article 7 of Directive 95/46[408] sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as being lawful". Moreover, "Member States cannot add new

403 Former Data Protection Directive, Art. 7 (f), now General Data Protection Regulation, Art. 6 (1) (f).

404 CJEU, Joined cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 November 2011.

405 Former Data Protection Directive, Art. 7 (f), now General Data Protection Regulation, Art. 6 (1) (f).

406 Former Data Protection Directive, now General Data Protection Regulation.

407 CJEU, Joined cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 November 2011, para. 28. See Data Protection Directive, Recitals 8 and 10.

408 Former Data Protection Directive, Art. 7, now General Data Protection Regulation, Art. 6 (1) (f).

principles relating to the lawfulness of the processing of personal data to Article 7 of the Directive 95/46[409] or impose additional requirements that have the effect of amending the scope of one of the six principles provided for" in Article 7.[410] The CJEU admitted that in relation to the balancing which is necessary pursuant to Article 7 (f) of Directive 95/46/EC, it is possible to take into consideration that the seriousness of the infringement of the data subject's fundamental rights resulting from the processing can vary, depending on whether or not the data in question already appear in public sources.

However, Article 7 (f) of the directive "precludes a Member State from excluding, in a categorical and generalised manner, the possibility of processing certain categories of personal data, without allowing the opposing rights and interests at issue to be balanced against each other in a particular case."

In light of those considerations, the CJEU concluded that Article 7 (f) of the Directive 95/46[411] must be interpreted "as precluding national rules which, in the absence of the data subject's consent, and in order to allow such processing of that data subject's personal data as is necessary to pursue a legitimate interest of the data controller or of the third party or parties to whom those data are disclosed, require not only that the fundamental rights and freedoms of the data subject be respected, but also that the data should appear in public sources, thereby excluding, in a categorical and generalised way, any processing of data not appearing in such sources."[412]

Whenever personal data is processed under the 'legitimate interests' ground, the individual has the right to object at any time to the processing, on grounds relating to his or her particular situation, according to Article 21 (1) of the GDPR. The controller must stop the processing, unless it demonstrates compelling legitimate grounds to continue it.

409 Former Data Protection Directive, Art. 7, now General Data Protection Regulation, Art. 6.

410 *Ibid.*

411 Former Data Protection Directive, Art. 7 (f), now General Data Protection Regulation, Art. 6 (1) (f).

412 CJEU, Joined cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 November 2011, paras. 40, 44 and 48–49.

Regarding **CoE law**, similar formulations can be found in Modernised Convention 108[413] and the recommendations of the CoE. The Profiling Recommendation acknowledges the processing of personal data for profiling purposes as legitimate if necessary for the legitimate interests of others, "except where such interests are overridden by the fundamental rights and freedoms of the data subjects".[414] In addition, "the protection of the rights and freedoms of others" is mentioned in Article 8 (2) of the ECHR as one of the legitimate grounds to limit the right to data protection.

> Example: In *Y v. Turkey,*[415] the applicant was HIV positive. As he was unconscious during his arrival at the hospital, the ambulance crew informed the hospital staff that he was HIV positive. The applicant argued before the ECtHR that the disclosure of this information had violated his right to respect for private life. However, given the need to protect the safety of the hospital staff, sharing the information was not regarded as a breach of his rights.

4.1.2. Processing special categories of data (sensitive data)

CoE law leaves it to domestic law to lay down appropriate protections for using sensitive data, provided the conditions of Article 6 of Modernised Convention 108 are fulfilled, namely that appropriate safeguards complementing the other provisions of the Convention are enshrined in law. **EU law,** in Article 9 of the GDPR, contains a detailed regime for processing special categories of data (also called 'sensitive data'). These data reveal racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership as well as for processing genetic and biometric data for the purposes of uniquely identifying a natural person, and for data concerning health, a person's sex life or sexual orientation. The processing of sensitive data is prohibited in principle.[416]

413 Explanatory Report of Modernised Convention 108, para 46.

414 Council of Europe, Committee of Ministers (2010), Recommendation CM/Rec(2010)13 and explanatory memorandum on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 23 November 2010, Art. 3.4 (b) (Profiling Recommendation).

415 ECtHR, *Y v. Turkey*, No. 648/10, 17 February 2015.

416 Former Data Protection Directive, Art. 7 (f), now General Data Protection Regulation, Art. 9 (1).

There is, however, an exhaustive list of exemptions to this prohibition, which can be found in Article 9 (2) of the regulation and which amount to lawful grounds for processing sensitive data. These exemptions include situations where:

- the data subject explicitly consents to the data processing;
- processing is carried out by a non-profit body with political, philosophical, religious or trade union purposes in the course of its legitimate activities and only relates to its (former) members or to persons who have regular contact with it for such purposes;
- processing concerns data explicitly made public by the data subject;
- processing is necessary:
    - to carry out the obligations of, and to exercise the specific rights of, the controller or of the data subject in the employment, social security and social protection context;
    - to protect the vital interests of the data subject or another natural person (when the data subject cannot give consent);
    - to establish, exercise or defend legal claims or when courts act in their judicial capacity;
    - for preventative or occupational medicine purposes: "for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional";
    - for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
    - for public interest reasons in the area of public health; or
    - for substantial public interest reasons.

To process special categories of data, a contractual relationship with the data subject is thus not viewed as a legal basis for the legitimate processing of sensitive data, except for a contract with a health professional subject to the obligation of professional secrecy.[417]

Explicit consent of the data subject

Under **EU law**, the first possible ground for lawful processing of any data, irrespective of whether they are non-sensitive or sensitive data, is the consent of the data subject. In the case of sensitive data, such consent must be explicit. Union or Member State law may, however, provide that the prohibition on processing special categories of data may not be lifted by the individual.[418] This could be the case, for example, when processing involves unusual risks for the data subject.

Employment law or social security and social protection law

Under **EU law**, the prohibition of Article 9 paragraph 1 can be lifted if the processing is necessary for carrying out obligations or rights of the controller or the data subject in the field of employment or social security. However, the processing needs to be authorised by EU law, national law or a collective agreement under national law, which provide appropriate safeguards for the fundamental rights and interests of the data subject.[419] Employment records held by an organisation may include sensitive personal data under certain conditions specified in the GDPR and relevant national law. Examples of sensitive data may include trade union membership or health information.

Vital interests of the data subject or another person

Under **EU law**, as in the case for non-sensitive data, sensitive data may be processed because of the vital interests of the data subject or another natural person.[420] Where processing is based on the vital interests of another person, this legitimate ground may only be invoked if such processing "cannot be manifestly based on another legal basis".[421] In some cases, processing personal data may protect both individual

417 General Data Protection Regulation, Art. 9 (2) (h) and (i).

418 *Ibid.,* Art. 9 (2) (a).

419 General Data Protection Regulation, Art. 9 (2) (b).

420 *Ibid.*, Art. 9 (2) (c).

421 *Ibid.*, Recital 46.

and public interests, for instance when processing is necessary for humanitarian purposes.[422]

For the processing of sensitive data to be legitimate on this basis, it would have to be impossible to ask the data subject for consent, because, for example, the data subject was unconscious or was absent and could not be reached. In other words, the person was physically or legally incapable of giving consent.

Charities or not-for-profit bodies

Processing personal data is also allowed in the course of the legitimate activities of foundations, associations or other non-profit-seeking bodies with a political, philosophical, religious or trade union aim. However, the processing must relate solely to the members or former members of the body, or to those who have regular contact with the body.[423] The sensitive data cannot be disclosed outside of those bodies without the data subject's consent.

Data manifestly made public by the data subject

Article 9 (2) (e) of the GDPR provides that processing is not prohibited if it relates to data which are manifestly made public by the data subject. Even though the meaning of "manifestly made public by the data subject" is not defined in the regulation, since it is an exception to prohibiting sensitive data processing, it must be construed strictly and as requiring the data subject to deliberately make his or her personal data public. Thus, where the television broadcasts a video taken from a video surveillance camera, showing, among other things, a firefighter getting injured trying to evacuate a building, it cannot be considered that the firefighter has manifestly made public the data. On the other hand, if the firefighter decides to describe the incident and publish the video and photos on a public internet page, he or she would have made a deliberate, affirmative act to make the personal data public. It is important to note that making one's data public does not constitute consent, but it is another permission for processing special categories of data.

The fact that the data subject had made public the processed personal data does not exempt controllers from their obligations under data protection law. For instance,

422 *Ibid.*

423 *Ibid.,* Art. 9 (2) (d).

the principle of purpose limitation continues to apply to personal data even if such data have been made publicly available.[424]

Legal claims

The processing of special categories of data which "is necessary for the establishment, exercise or defence of legal claims", whether in court proceedings or in an administrative or out-of-court procedure,[425] is also allowed under the GDPR.[426] In this case, processing must be relevant to a specific legal claim and its exercise or defence respectively, and may be requested by any one of the disputing parties.

When acting in their judicial capacity, courts may process special categories of data within the context of resolving a legal dispute.[427] Examples of these special categories of data processed in this context could include for example, genetic data when establishing parentage, or health status when part of the evidence concerns details of an injury sustained by a victim of crime.

Reasons of substantial public interest

According to Article 9 (2) (g) of the GDPR, Member States may introduce further circumstances in which sensitive data may be processed, as long as:

- processing data is for reasons of substantial public interest;
- it is provided for by European or national law;
- the European or national law is proportionate, respects the right to data protection and provides suitable and specific measures to safeguard the rights and interests of the data subject.[428]

A prominent example are electronic health file systems. Such systems permit health data, collected by health care providers in the course of treating a patient, to be

424 Article 29 Working Party (2013), *Opinion 3/13 on purpose limitation*, WP 203, Brussels, 2 April 2013, p. 14.

425 General Data Protection Regulation, Preamble Recital 52.

426 *Ibid*., Art. 9 (2) (f).

427 *Ibid*.

428 *Ibid*., Art. 9 (2) (g).

made available to other health care providers of this patient on a large scale, usually nationwide.

The Article 29 Working Party concluded that the establishment of such systems could not occur under existing legal rules for processing data about patients.[429] However, it is possible for electronic health file systems to exist if they are based on "reasons of substantial public interest".[430] This would require an explicit legal basis for their establishment, which would also contain the necessary safeguards to ensure that the system is run securely.[431]

Other grounds for processing of sensitive data

The GDPR provides that sensitive data can be processed where processing is necessary for:[432]

- preventative or occupational medicine purposes, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services on the basis of EU or Member State law, or pursuant to a contract with a health professional;

- reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or Member State law. The law must provide for suitable and specific measures to safeguard the rights of the data subject;

- archiving, scientific or historical research or statistical purposes on the basis of Union or Member State law. The law must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for appropriate and specific measures to safeguard the rights and interests of the data subject.

429 Article 29 Working Party (2007), *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, WP 131, Brussels, 15 February 2007. See also General Data Protection Regulation, Art. 9 (3).

430 General Data Protection Regulation, Art. 9 (2) (g).

431 Article 29 Working Party (2007), *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, WP 131, Brussels, 15 February 2007.

432 General Data Protection Regulation, Art. 9 (2) (h), (i) and (j).

Additional conditions under national law

The GDPR also allows Member States to introduce or maintain additional conditions, including limitations for processing genetic, biometric and health-related data.[433]

4.2. Rules on security of processing

Key points

- The rules on security of processing obligate the controller and the processor to implement appropriate technical and organisational measures to prevent any unauthorised interference with data processing operations.
- The necessary level of data security is determined by:
  - the security features available in the market for any particular type of processing;
  - the costs;
  - the risks of processing the data for fundamental rights and freedoms of data subjects.
- Ensuring confidentiality of personal data is part of a general principle recognised in the General Data Protection Regulation.

Under both **EU and CoE law**, controllers have the general obligation to be transparent and accountable when processing personal data, and, in particular, about data breaches where such breaches occur. In case of personal data breaches, controllers must notify the supervisory authorities, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Data subjects should also be informed about the personal data breach when it is likely to result in a high risk to the rights and freedoms of natural persons.

4.2.1. Elements of data security

According to the relevant provisions in **EU law**:

> *"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk*

433 *Ibid.*, Art. 9 (2) (h) and 9 (4).

> *of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk [...].*"[434]

These measures include, among others:

- pseudonymising and encrypting personal data;[435]
- ensuring that the processing system and service maintain confidentiality, integrity, availability and resilience;[436]
- restoring the availability of and access to personal data in the event of data loss in a timely manner;[437]
- a process for testing, assessing and evaluating the effectiveness of the measures to ensure the security of processing.[438]

A similar provision exists under **CoE law**:

> *"Each Party shall provide that the controller and, where applicable, the processor takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data."*[439]

Under **EU and CoE law**, a data breach that may have an impact on the rights and freedoms of individuals obliges the controller to notify the supervisory authority of the breach (see Section 4.2.3).

Often, there are also industrial, national and international standards which have been developed for safe data processing. The European Privacy Seal (EuroPriSe), for instance, is an eTEN (Trans-European Telecommunications Networks) project of

434 *Ibid.*, Art. 32 (1).
435 *Ibid.*, Art. 32 (1) (a).
436 *Ibid.*, Art. 32 (1) (b).
437 *Ibid.*, Art. 32 (1) (c).
438 *Ibid.*, Art. 32 (1) (d).
439 Modernised Convention 108, Art. 7 (1).

the EU which explores the possibilities of certifying products, especially software, as facilitating compliance with European data protection law. The European Network and Information Security Agency (ENISA) was set up to enhance the ability of the EU, the EU Member States and the business community to prevent, address and respond to network and information security problems.[440] ENISA regularly publishes analyses of current security threats and advice on how to address them.[441]

Data security is not just achieved by having the right equipment – hardware and software – in place. It also requires appropriate internal organisational rules. Such internal rules would ideally cover the following issues:

- regular provision of information to all employees about data security rules and their obligations under data protection law, especially regarding their confidentiality obligations;
- clear distribution of responsibilities and a clear outline of competences in matters of data processing, especially regarding decisions to process personal data and to transmit data to third parties or to data subjects;
- use of personal data only according to the instructions of the competent person or according to generally laid down rules;
- protection of access to locations and to hard- and software of the controller or processor, including checks on authorisation for access;
- ensuring that authorisations to access personal data have been assigned by the competent person and require proper documentation;
- automated protocols on electronic access to personal data and regular checks of such protocols by the internal supervisory desk (therefore requiring all data processing activities to be recorded);
- careful documentation for other forms of disclosure than automated access to data so as to demonstrate that no illegal data transmissions have taken place.

440 Regulation (EC) No. 526/2013of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No. 460/, OJ 2013 L 165.

441 For example, ENISA, (2016), Cyber Security and Resilience of smart cars. Good practices and recommendations; ENISA (2016), Security of Mobile Payments and Digital Wallets.

Offering adequate data security training and education to staff members is also an important element of effective security precautions. Verification procedures must also be put in place to ensure that appropriate measures not only exist on paper but are implemented and work in practice (such as internal or external audits).

Measures for improving the security level of a controller or processor include instruments such as personal data protection officials, security education of employees, regular audits, penetration tests and quality seals.

> Example: In *I v. Finland*,[442] the applicant was unable to prove that her health records had been accessed illegitimately by other employees of the hospital where she worked. Her claim of a violation of her right to data protection was, therefore, rejected by the domestic courts. The ECtHR concluded that there had been a violation of Article 8 of the ECHR, as the hospital's register system for health files "was such that it was not possible to retroactively clarify the use of patient records as it revealed only the five most recent consultations and that this information was deleted once the file had been returned to the archives". For the Court, it was decisive that the records system in place in the hospital had clearly not been in accordance with the legal requirements contained in domestic law, a fact that was not given due weight by the domestic courts.

The EU has put in place the Directive on security of network and information systems (the NIS Directive),[443] which is the first EU-wide legal instrument on cybersecurity. The Directive aims to improve cybersecurity at national level on the one hand, and to increase the level of cooperation within the EU on the other. It also imposes obligations on operators of essential services (including operators in the sectors of energy, health, banking, transport, digital infrastructure, etc.) and digital services providers to manage risks, ensure the security of their network and information systems, and report security incidents.

442 ECtHR, *I v. Finland*, No. 20511/03, 17 July 2008.

443 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ 2016 L 194.

Outlook

In September 2017, the European Commission proposed a draft regulation aimed at reforming ENISA's mandate, to take into account the agency's new competences and responsibilities under the NIS Directive. The objective of the proposed regulation is to develop ENISA's tasks and reinforce its role as the "reference point in the EU cybersecurity ecosystem".[444] The proposed regulation should be without prejudice to the GDPR principles, and by clarifying the necessary elements composing the European cybersecurity certification schemes, should also strengthen the security of personal data. In parallel, in September 2017, the European Commission proposed a draft implementing regulation specifying the elements that digital service providers shall take into account to ensure that their network and information systems are secure, as requested by Article 16 (8) of the NIS Directive. At the time of drafting of the handbook, discussions on these two proposals were ongoing.

4.2.2. Confidentiality

Under EU law, the GDPR recognises confidentiality of personal data as part of a general principle.[445] Providers of publicly available electronic communications services need to ensure confidentiality. They are also under obligation to safeguard the security of their services.[446]

> Example: An employee of an insurance company receives a telephone call at her workplace from someone who says he is a client, requiring information concerning his insurance contract.
>
> The duty to keep clients' data confidential requires that the employee apply at least minimum security measures before disclosing personal data. This could be done, for example, by offering to return the call to a telephone number documented in the client's file.

Pursuant to Article 5 (1) (f), personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against

444 Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (Cybersecurity Act), COM(2017)477, 13 September 2017, p. 6.

445 General Data Protection Regulation, Art. 5 (1) (f).

446 Directive on privacy and electronic communications, Art. 5 (1).

unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

By virtue of Article 32, the controller and the processor must implement technical and organisational measures to ensure a high level of security. Such measures include, among others, the pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the processing, the evaluation and testing of the effectiveness of the measures, and the ability to restore the processing in the event of a physical or technical incident. Additionally, adherence to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the principle of integrity and confidentiality. In addition, according to Article 28 of the GDPR, the contract binding the controller to the processor must stipulate that the processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

The duty of confidentiality does not extend to situations where data come to the knowledge of a person in his or her capacity as a private individual and not as an employee of a controller or processor. In this case, Articles 32 and 28 of the GDPR do not apply, as the use of personal data by private individuals is completely exempt from the regulation's remit where such use falls within the boundaries of the so-called household exemption.[447] The household exemption is the use of personal data "by a natural person in the course of purely personal or household activity".[448] Since the CJEU's decision in the case of *Bodil Lindqvist*,[449] this exemption must, however, be interpreted narrowly, especially regarding data disclosure. Particularly, the household exemption will not extend to the publication of personal data to an unlimited number of recipients on the internet, or to data processing that has professional or commercial aspects (for more details on the case, see Sections 2.1.2, 2.2.2 and 2.3.1).

"Confidentiality of communications" is another aspect of confidentiality, which is subject to *lex specialis*. The special rules for ensuring confidentiality of electronic communications under the e-Privacy Directive require Member States to prohibit

447 General Data Protection Regulation, Art. 2 (2) (c).

448 *Ibid.*

449 CJEU, C-101/01, *Criminal proceedings against Bodil Lindqvist*, 6 November 2003.

any persons other than users, or without the consent of the users, from listening, tapping, storage or other kinds of interception or surveillance of communications and the related metadata.[450] National law may authorise exceptions from this principle only for reasons of national security, defence, prevention or detection of crimes, and only if such measures are necessary and proportionate for the aims pursued.[451] The same rules will apply under the future e-Privacy Regulation, yet the scope of the legal act on e-Privacy will be extended from publicly available electronic communications services to also cover communications done through over-the-top services (such as mobile applications).

Under CoE law, the obligation of confidentiality is implied in the notion of data security in Article 7 (1) of Modernised Convention 108, which deals with data security.

For processors, confidentiality means that they may not disclose the data to third parties or other recipients without authorisation. For the employees of a controller or processor, confidentiality requires that they use personal data only according to the instructions of their competent superiors.

The obligation of confidentiality must be included in any contract between controllers and their processors. In addition, controllers and processors will have to take specific measures to establish a legal duty of confidentiality for their employees, normally achieved by including confidentiality clauses in the employee's employment contract.

Infringement of the professional duty of confidentiality is punishable under criminal law in many EU Member States and Parties to Convention 108.

4.2.3. Personal data breach notifications

A personal data breach refers to a security breach leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to processed personal data.[452] While new technologies, such as encryption, now provide for more possibilities to ensure the security of processing, data breaches are still a common phenomenon. The causes of data breaches may range from accidental

450 Directive on privacy and electronic communications, Art. 5 (1).

451 *Ibid*., Art. 15 (1).

452 General Data Protection Regulation, Art. 4 (12); See also Article 29 Working Party (2017), *Guidelines on Personal data breach notification under Regulation 2016/679*, WP250, 3 October 2017, p. 8.

mistakes by people working inside an organisation to external threats such as hackers and cybercriminal organisations.

Data breaches can be very detrimental to the privacy and data protection rights of individuals who, as a result of the breach, lose control over their personal data. Breaches may lead to identity theft or fraud, financial loss or material damages, loss of confidentiality of personal data protected by professional secrecy, and damage to the data subject's reputation. In its Guidelines on Personal data breach notification under Regulation 2016/679, the Article 29 Working Party explains that breaches may have three types of impact on personal data: disclosure, loss, and/or alteration.[453] In addition to the obligation to take measures to ensure the security of processing, as explained in Section 4.2, it is equally important to ensure that when breaches occur, controllers address them in an appropriate and timely manner.

Supervisory authorities and individuals are often unaware of the occurrence of a data breach and this prevents individuals from taking steps to protect themselves from its negative consequences. To affirm the rights of individuals and limit the impact of data breaches, the **EU and CoE** impose a notification requirement on controllers in certain circumstances.

Under the **CoE** Modernised Convention 108, Contracting Parties must, as a minimum, require controllers to notify the competent supervisory authority of data breaches that may seriously interfere with the rights of the data subjects. Such notification should be completed 'without delay'.[454]

EU law establishes a detailed regime regulating the timing and content of the notifications.[455] Accordingly, controllers must notify certain data breaches to the supervisory authorities without undue delay and, where feasible, within 72 hours of the moment they become aware of the breach. If they exceed the 72-hour timeframe, the notification needs to be accompanied with an explanation for the delay. Controllers are exempt from the notification requirement only where they are able to demonstrate that the data breach is unlikely to result in a risk to the rights and freedoms of the individuals concerned.

453 Article 29 Working Party (2017), *Guidelines on Personal data breach notification under Regulation 2016/679*, WP250, 3 October 2017, p. 6.

454 Modernised Convention 108, Art. 7 (2); Explanatory Report of Modernised Convention 108, paras. 64-66.

455 General Data Protection Regulation, Art. 33 and 34.

The regulation specifies the minimum information to be included in the notification to allow the supervisory authority to take the necessary action.[456] The notification must include, at least, a description of the nature of the data breach and of the categories and approximate numbers of data subjects affected, a description of the possible consequences of the breach and of the measures implemented by the controller to address and mitigate its consequences. In addition, the name and contact details of the data protection officer or another contact point should be provided, to enable the competent supervisory authority to obtain further information if necessary.

If a data breach is likely to cause high risks to the rights and freedoms of individuals, controllers must inform these individuals (the data subjects) of the breach without undue delay.[457] The information to the data subjects, including the description of the data breach, must be drafted in clear and plain language, and include information similar to that required for notifications to supervisory authorities. In certain circumstances, controllers may be exempt from the obligation to notify data subjects of such breaches. Exemptions apply where the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption. Action taken by the controller after the breach to ensure that the harm to the rights of data subjects will no longer materialise may also exempt the controller from the obligation to notify the data subjects. Finally, if notification entails disproportionate effort on behalf of the controller, data subjects can be informed about the breach through other means, such as a public communication or similar measures.[458]

The obligation to notify data breaches to the supervisory authorities and data subjects is addressed to controllers. However, data breaches may occur irrespective of whether processing is carried out by a controller or processor. For this reason, it is essential to ensure that processors are also required to report data breaches. In this case, processors must notify data breaches to the controller without undue delay.[459] The controller is then responsible for notifying the supervisory authorities and the data subjects affected, subject to the aforementioned rules and timeframe.

456 *Ibid.*, Art. 33 (3).

457 *Ibid.*, Art. 34.

458 *Ibid.*, Art. 34 (3) (c).

459 *Ibid.*, Art. 33 (2).

4.3. Rules on accountability and promoting compliance

Key points

- To ensure accountability in the processing of personal data, controllers and processors must maintain records of the processing activities carried out under their responsibility and provide them to the supervisory authorities where requested.
- The General Data Protection Regulation sets out several instruments for promoting compliance:
  - the appointment of data protection officers in certain situations;
  - the conducting of an impact assessment before the start of processing activities which are likely to pose high risks to the rights and freedoms of individuals;
  - prior consultation of the relevant supervisory authority if the impact assessment indicates that processing presents risks that cannot be mitigated;
  - codes of conduct for controllers and processors specifying the application of the regulation in various processing sectors;
  - certification mechanisms, seals and marks.
- CoE law proposes similar instruments for promoting compliance in Modernised Convention 108.

The principle of accountability is particularly important to guarantee the enforcement of the data protection rules in Europe. The controller is responsible for, and must be able to demonstrate, compliance with data protection rules. Accountability should not only come into play after a violation has occurred. Rather, controllers have a proactive obligation to follow adequate data management policies at all stages of data processing. European data protection law requires controllers to implement technical and organisational measures to ensure, and be able to demonstrate, that processing is carried out in accordance with the law. Among these measures is the appointment of data protection officers, the keeping of records and documentation related to the processing, and the conduct of privacy impact assessments.

4.3.1. Data Protection Officers

Data Protection Officers (DPOs) are persons who advise on compliance with data protection rules in organisations undertaking data processing. They are 'a cornerstone of accountability' since they facilitate compliance, while also acting as intermediaries between the supervisory authorities, data subjects and the organisation by which they have been appointed.

Under CoE law, Article 10 (1) of Modernised Convention 108 places a general accountability responsibility on controllers and processors. This requires controllers and processors to take all appropriate measures to comply with the data protection rules stipulated in the convention, and to be able to demonstrate that the data processing under their control complies with the provisions of the convention. Even though the convention does not specify the concrete measures that controllers and processors should adopt, the Explanatory Report of Modernised Convention 108 indicates that the appointment of a DPO would be one possible measure to help demonstrate compliance. DPOs should be provided with all means necessary to fulfil their mandates.[460]

Contrary to CoE law, **in the EU**, the appointment of a DPO is not always at the discretion of controllers and processors but is mandatory in certain conditions. The GDPR recognises the DPO as playing a key role in the new governance system and includes detailed provisions regarding the officer's appointment, position, duties and tasks.[461]

The GDPR makes appointing a DPO mandatory in three specific cases: where a public authority or body carries out the processing; where the controller's or processor's core activities consist of processing operations which require the regular and systematic monitoring of data subjects on a large scale or where the core activities consist of large-scale processing of special categories of data or personal data relating to criminal convictions and offences.[462] Even though terms such as 'systematic monitoring on a large scale' and 'core activities' are not defined in the regulation, the Article 29 Working Party has issued guidelines on how they should be interpreted.[463]

460 Explanatory Report of Modernised Convention 108, para. 87.

461 General Data Protection Regulation, Art. 37–39.

462 *Ibid*., Art. 37 (1).

463 Article 29 Working Party (2017), *Guidelines on Data Protection Officers ('DPOs')*, WP 243 rev.01, last revised and adopted 5 April 2017.

Example: Social media companies and search engines are likely to be considered controllers whose processing operations require the regular and systematic monitoring of data subjects on a large scale. The business model of such companies is based on the processing of large amounts of personal data, and they generate significant revenue through offering targeted advertising services and by allowing companies to advertise on the sites. Targeted advertising is a way of placing advertisements based on demographics and the consumers' previous buying history or behaviour. It therefore requires the systematic monitoring of the data subjects' online habits and behaviour.

Example: A hospital and a healthcare insurance company are typical examples of controllers whose activities consist of large scale processing of special categories of personal data. Data revealing information concerning the health of an individual constitute special categories of personal data under both CoE and EU law, thus meriting enhanced protection. EU law further recognises genetic and biometric data as special categories. Insofar as medical establishments and insurance companies process such data on a large scale, they are required under the GDPR to appoint a data protection officer.

Additionally, Article 37 (4) of the GDPR provides that in cases other than the three mandatory ones required under Article 37 (1), the controller, processor or associations and other bodies representing categories of controllers or processors may, or where required by Union or Member State law shall, designate a data protection officer.

All other organisations are not legally obliged to designate a DPO. However, the GDPR provides that controllers and processors may choose to voluntarily designate a DPO, while also allowing the possibility for Member States to make such designation mandatory for more types of organisations than those foreseen under the regulation.[464]

Once a controller appoints a DPO, they must ensure that he or she "is involved, properly and in a timely manner, in all issues which relate to the protection of personal data" within the organisation.[465] For instance, DPOs should be involved in providing advice on carrying out data protection impact assessments, and in creating and keeping records of processing activities in an organisation. To enable DPOs to

464 General Data Protection Regulation, Art. 37 (3) and (4).

465 *Ibid*., Art. 38 (1).

effectively carry out their tasks, controllers and processors must provide them with the necessary resources, including financial resources, infrastructure and equipment. Additional requirements, include providing DPOs with sufficient time to fulfil their functions and continuous training to enable them to develop their expertise and stay up to date with all developments in data protection law.[466]

The GDPR establishes some basic guarantees to ensure that DPOs act in an independent manner. Controllers and processors must ensure that in exercising their tasks related to data protection, DPOs do not receive any instructions from the company, including persons at the highest management level. In addition, they must not be dismissed or penalised in any way for performing their tasks.[467] Take, for example, a case where the DPO advises a controller or processor to conduct a data protection impact assessment because he or she considers that the processing is likely to result in high risk for data subjects. The company disagrees with the DPO's advice, does not consider it to be well-founded and consequently decides not to proceed with an impact assessment. The company can ignore the advice but cannot dismiss or penalise the DPO for providing it.

Finally, the tasks and duties of DPOs are detailed in Article 39 of the GDPR. These include the requirements to inform and advise the companies and employees carrying out the processing of their obligations pursuant to the legislation and to monitor compliance with EU and national data protection rules, through carrying out audits and training staff involved in processing operations. DPOs must also cooperate with the supervisory authority and act as the contact point for the latter on matters related to data processing, such as, for instance, a data breach.

Concerning the personal data handled by EU institutions and bodies, Regulation 45/2001 provides that each Union institution and body must appoint a DPO. The DPO is entrusted with ensuring that the provisions of the regulation are correctly applied within the EU institutions and bodies and that both data subjects and data controllers are informed of their rights and obligations.[468] He or she is also responsible for responding to requests from the EDPS and cooperating with him or her where needed. Similarly to the GDPR, Regulation 45/2001 contains provisions on the independence of DPOs in carrying out their tasks, and the need to provide them

466 Article 29 Working Party (2017), *Guidelines on Data Protection Officers ('DPOs')*, WP 243 rev.01, last revised and adopted 5 April 2017, para. 3.1.

467 General Data Protection Regulation, Art. 38 (2) and (3).

468 See Art. 24 (1) of Regulation (EC) No. 45/2001 for the complete list of tasks of DPOs.

with the necessary staff and resources.[469] DPOs must be notified before an EU institution or body (or of departments of these organisations) carries out any processing operations and they must keep a register of all notified processing operations.[470]

4.3.2. Records of processing activities

To be able to demonstrate compliance and to be held accountable, companies are often legally required to document and record their activities. An important example is tax law and auditing, which require all companies to maintain extensive documentation and record-keeping. Establishing similar requirements in other fields of law, in particular data protection law, is also important, as record-keeping is an important way to facilitate compliance with data protection rules. **EU law** thus provides that controllers, or their representatives, must maintain a record of the processing activities carried out under their responsibility.[471] This obligation is intended to ensure that, if necessary, supervisory authorities will have the necessary documentation to enable them to confirm the lawfulness of processing.

The information to be documented includes the following:

- name and contact details of the controller, and of the joint controller, the controller's representative and the DPO, where applicable;
- purposes of the processing;
- description of the categories of data subjects and of the categories of personal data related to the processing;
- information on the categories of recipients to whom personal data have been, or will be, disclosed;
- information on whether transfers of personal data to third countries or international organisations have been, or will be, carried out;
- where possible, the time limits foreseen for the deletion of the different categories of personal data, as well as an overview of the technical measures adopted to ensure the security of processing.[472]

469 Regulation (EC) No. 45/2001, Art. 24 (6) and (7).

470 *Ibid.*, Art. 25 and 26.

471 General Data Protection Regulation, Art. 30.

472 *Ibid.*, Art. 30 (1).

The obligation to keep records of processing activities under the GDPR concerns not only controllers, but also processors. This is an important development as, prior to the adoption of the regulation, the contract concluded between the controller and the processor primarily covered the processor's obligations. Their record-keeping obligation is now directly foreseen under law.

The GDPR provides for an exception from this obligation. The requirement to keep records does not apply to an enterprise or organisation (controller or processor) which employs fewer than 250 persons. The exception is, however, subject to the requirements that the organisation concerned does not undertake processing likely to result in a risk to the rights and freedoms of data subjects, that processing is only occasional and that it does not include special categories of data as referred to in Article 9 (1) or personal data relating to criminal convictions and offences referred to in Article 10.

Maintaining records of processing activities should enable controllers and processors to demonstrate compliance with the regulation. It should also enable supervisory authorities to monitor the lawfulness of processing. Where a supervisory authority requests access to those records, controllers and processors are obliged to cooperate and make them available.

4.3.3. Data protection impact assessment and prior consultation

Processing operations present some inherent risks to the rights of individuals. Personal data may be lost, disclosed to unauthorised parties or processed in an unlawful manner. Naturally, risks vary depending on the nature and scope of processing. Large-scale operations involving the processing of sensitive data, for example, have a much higher degree of risk for data subjects compared to the potential risks when a small company processes its employees' addresses and personal phone numbers.

As new technologies emerge and processing becomes increasingly complex, controllers must address such risks by examining the likely impact of the intended processing before starting the processing operation. This enables organisations to properly identify, address and mitigate the risks in advance, significantly limiting the likelihood of a negative impact on individuals as a result of the processing.

Data protection impact assessments are foreseen **under both CoE and EU law**. In the CoE legal framework, Article 10 (2) of Modernised Convention 108 requires Contracting Parties to ensure that controllers and processors "examine the likely impact

of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing" and, following the assessment, design the processing in such a manner as to prevent or minimise the risks linked to the processing.

EU law imposes a similar, more detailed, obligation on controllers falling within the scope of the GDPR. Article 35 provides that an impact assessment must be carried out where processing is likely to result in a high risk to the rights and freedoms of individuals. The regulation does not define how the likelihood of risk is to be assessed but, rather, indicates what those risks might be.[473] It contains a list of processing operations considered high risk and for which a prior impact assessment is particularly necessary, namely in cases where:

- personal data are processed for making decisions concerning natural persons, following any systematic and extensive evaluation of personal aspects relating to the individuals (profiling);
- sensitive data or personal data relating to criminal convictions and offences are processed on a large scale;
- processing involves the large-scale, systematic monitoring of publicly accessible areas.

The supervisory authorities must adopt and publish a list of the kind of processing operations that need to be subject to impact assessments. They may also establish a list of processing operations exempted from this obligation.[474]

Where an impact assessment is required, controllers must assess the necessity and proportionality of the processing and the possible risks to the rights of individuals. The impact assessment must also contain the planned security measures to address the risks identified. To establish the lists, the Member States' supervisory authorities are required to cooperate with each other and with the European Data Protection Board. This will ensure a consistent approach across the EU to those operations requiring an impact assessment and controllers will face similar requirements irrespective of their location.

473 General Data Protection Regulation, Preamble, Recital 75.

474 *Ibid*., Art. 35 (4) and (5).

If, following an impact assessment, it appears that the processing will result in high risk for the rights of individuals and no measures were introduced to mitigate the risk, the controller must consult the relevant supervisory authority before starting the processing operation.[475]

The Article 29 Working Party has issued guidelines on data protection impact assessments and how to determine whether or not processing is likely to result in high risk.[476] It developed nine criteria to help to determine whether a data protection impact assessment is required in a specific case:[477] (1) evaluation or scoring; (2) automated decision-making with legal or similar significant effect; (3) systematic monitoring; (4) sensitive data; (5) data processed on a large scale; (6) datasets that have been matched or combined; (7) data concerning vulnerable data subjects; (8) innovative use or applying technological or organisational solutions; (9) when the processing in itself "prevents data subjects from exercising a right or using a service or a contract". The Article 29 Working Party introduced the rule of thumb that processing operations which meet fewer than two criteria pose lower risk levels and do not require a data protection assessment, whereas those which meet two or more criteria will require such an assessment. In cases where it is unclear whether a data protection impact assessment is required, the Article 29 Working Party recommends carrying out such an assessment because it is "a useful tool to help data controllers comply with data protection law".[478] Where a new data processing technology is introduced, it is important that a data protection impact assessment is carried out.[479]

4.3.4. Codes of conduct

Codes of conduct are meant to be used in several industry sectors, to outline and specify the application of the GDPR in their specific sectors. For controllers and processors of personal data, creating such codes may greatly improve compliance and enhance the implementation of EU data protection rules. The expertise of the members of the sector will favour finding solutions which are practical and, therefore,

475 *Ibid*., Art. 36 (1); Article 29 Working Party (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, Brussels, 4 October 2017.

476 Article 29 Working Party (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, Brussels, 4 October 2017.

477 *Ibid*., pp. 9–11.

478 *Ibid*., p. 9.

479 *Ibid*.

likely to be followed. Acknowledging the importance of such codes in the effective application of the data protection law, the GDPR calls on Member States, the supervisory authorities, the Commission and the European Data Protection Board to encourage the drawing up of codes of conduct intended to contribute to the proper application of the regulation across the EU.[480] The codes could specify application of the regulation in specific sectors, including matters such as the collection of personal data, the information to be provided to data subjects and to the public, and the exercise of the rights of data subjects.

To ensure that the codes of conduct comply with the rules established under the GDPR, the codes must be submitted to the competent supervisory authority before being adopted. The supervisory authority then provides an opinion on whether the draft code provided furthers compliance with the regulation and, if it finds that the code provides appropriate safeguards, it approves the code.[481] Supervisory authorities must publish the approved codes of conduct as well as the criteria upon which their approval was based. Where a draft code of conduct relates to processing activities in several Member States, the competent supervisory authority, before approving the draft code, amendment or extension, shall submit the code to the European Data Protection Board which shall provide an opinion on the compliance of the code with the GDPR. The Commission may, by way of implementing acts, decide that the approved code of conduct submitted to it has general validity within the Union.

Adherence to a code of conduct offers important advantages to both data subjects and controllers and processors. Such codes provide detailed guidance which tailors legal requirement to specific sectors and furthers the transparency of processing activities. Controllers and processors may also use adherence to the codes as demonstrable evidence of their compliance with EU law and as a means of boosting their public image as organisations that prioritise and commit to data protection in their operations. Approved codes of conduct, together with binding and enforceable commitments, might be used as appropriate safeguards to transfer data to third countries. To ensure that organisations adhering to the codes of conduct indeed comply with it, a special body (accredited by the relevant supervisory authority) may be appointed to monitor and ensure compliance. To effectively fulfil its tasks, the body must be independent, have proven expertise on the matters regulated by the code of conduct, and have transparent procedures and structures to enable it to handle complaints about infringements of the code.[482]

480 General Data Protection Regulation, Art. 40 (1).

481 *Ibid.*, Art. 40 (5).

482 *Ibid.*, Art. 41 (1) and (2).

Under **CoE law**, Modernised Convention 108 provides that the level of data protection guaranteed by national law may be usefully reinforced by voluntary regulation measures, such as codes of good practice or codes of professional conduct. However, these only constitute voluntary measures under Modernised Convention 108: one cannot derive any legal obligation to put such measures in place, although it is advisable, and such measures are not, by themselves, sufficient to ensure full compliance with the convention.[483]

4.3.5. Certification

In addition to codes of conduct, certification mechanisms and data protection seals and marks are another means by which controllers and processors can demonstrate compliance with the GDPR. To this end, the regulation provides for a voluntary certification system, whereby certain bodies or supervisory authorities may issue certifications. Controllers and processors opting to adhere to a certification mechanism may gain more visibility and credibility, as certifications, seals and marks allow data subjects to quickly assess an organisations' level of protection for data processing. Importantly, the fact that a controller or processor possesses such a certification does not reduce its duties and responsibilities to comply with all the requirements of the regulation.

4.4. Data protection by design and by default

Data protection by design

EU law requires that controllers put in place measures to effectively implement data protection principles and to integrate the necessary safeguards to meet the requirements of the regulation and protect the rights of data subjects.[484] These measures should be implemented both at the time of processing and when determining the means for processing. In implementing these measures, the controller needs to take into account the state of the art, the costs of implementation, the nature, scope and purposes of personal data processing and the risks and severity for the rights and freedoms of the data subject.[485]

483 Explanatory Report of Modernised Convention 108, para. 33.

484 General Data Protection Regulation, Art. 25 (1).

485 See Article 29 Working Party (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, 4 October 2017. See also ENISA (2015), Privacy and Data Protection by Design-from policy to engineering, 12 January 2015.

CoE law requires that controllers and processors assess the likely effect of processing personal data on the rights and freedoms of the data subjects before beginning the processing. In addition, controllers and processors are obliged to design the data processing in such a way as to prevent or minimise the risk of interference with those rights and freedoms, and implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.[486]

Data protection by default

EU law requires that the controller implements appropriate measures to ensure that only personal data which are necessary for the purposes will be processed by default. This obligation applies to the amount of personal data collected, the extent of the processing, the storage period and accessibility.[487] Such a measure must ensure, for example, that not all the controllers' employees have access to the subjects' personal data. Further guidance was developed by the EDPS in the *Necessity Toolkit*.[488]

CoE law requires that controllers and processors implement technical and organisational measures to consider the implications of the right to data protection, and implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.[489]

In 2016, ENISA published a report on available privacy tools and services.[490] Amongst other considerations, this assessment provides an index of criteria and parameters which are indicators of good or poor privacy practices. Whereas some criteria relate directly to provisions of the GDPR – such as the use of pseudonymisation, and of approved certification mechanisms – others provide innovative initiatives to ensure privacy by design and by default. For instance, the criterion of usability, while not directly related to privacy, may enhance privacy, since it can enable the broader adoption of a privacy tool or service. Indeed, privacy tools that

486 Modernised Convention 108, Art. 10 (2) and (3), Explanatory Report of Modernised Convention 108, para 89.

487 General Data Protection Regulation, Art. 25 (2).

488 European Data Protection Supervisor (EDPS), (2017), *Necessity Toolkit*, Brussels, 11 April 2017.

489 Modernised Convention 108, Art. 10 (3), Explanatory Report of Modernised Convention 108, para. 89.

490 ENISA, PETs controls matrix: A systematic approach for assessing online and mobile privacy tools, 20 December 2016.

are difficult to implement in practice may have very low adoption levels by the general public, even if they offer very strong privacy guarantees. Additionally, the criterion of the maturity and stability of the privacy tool – meaning the way that a tool evolves over time and responds to existing or new challenges related to privacy – is of crucial importance. Other privacy enhanced technologies, for example, in the context of secure communications, include end-to-end encryption (communication where the only people who can read the messages are the people communicating); client-server encryption (encrypting the communication channel established between a client and a server); authentication (verification of communicating parties' identities); and anonymous communication (no third party can identify the communicating parties).

5 Independent supervision

EU	Issues covered	CoE
The Charter, Article 8 (3) Treaty on the Functioning of the EU, Article 16 (2) General Data Protection Regulation, Articles 51–59 CJEU, C-518/07, *European Commission v. Federal Republic of Germany* [GC], 2010 CJEU, C-614/10, *European Commission v. Republic of Austria* [GC], 2012 CJEU, C-288/12, *European Commission v. Hungary* [GC], 2014 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 2015	**Supervisory authorities**	Modernised Convention 108, Article 15
General Data Protection Regulation, Articles 60–67	**Cooperation between supervisory authorities**	Modernised Convention 108, Articles 16–21
General Data Protection Regulation, Articles 68–76	**European Data Protection Board**	

Key points

- Independent supervision is an essential component of European data protection law and is enshrined in Article 8 (3) of the Charter.
- To ensure effective data protection, independent supervisory authorities must be established under national law.
- Supervisory authorities must act with complete independence, which must be guaranteed by the founding law and reflected in the specific organisational structure of the supervisory authority.
- Supervisory authorities have specific powers and tasks. These include, among others, to:
  - monitor and promote data protection at the national level;
  - advise data subjects and controllers as well as the government and the public at large;
  - hear complaints and assist data subjects with alleged violations of data protection rights;
  - supervise controllers and processors.
- Supervisory authorities also have the power to intervene if necessary by:
  - warning, reprimanding or even fining controllers and processors;
  - ordering data to be rectified, blocked or deleted;
  - imposing a ban on processing or an administrative fine;
  - referring matters to court.
- As personal data processing often involves controllers, processors and data subjects located in different states, supervisory authorities are required to cooperate with one another on cross-border issues to ensure the effective protection of individuals in Europe.
- In the EU, the General Data Protection Regulation establishes a one-stop-shop mechanism for cross-border processing cases. Some companies conduct cross-border processing activities due to processing personal data in the context of activities of establishments in more than one Member State or in the context of a single establishment in the Union but which substantially affects data subjects in more than one Member State. Under the mechanism, such companies will only have to deal with one national data protection supervisory authority.
- A cooperation and consistency mechanism will allow for a coordinated approach between all the supervisory authorities involved in the case. The lead supervisory

authority – of the main or single establishment – will consult and submit its draft decision with the other concerned supervisory authorities.

- Similarly to the current Article 29 Working Party, the supervisory authority of each Member State and the European Data Protection Supervisor (EDPS) will be part of the European Data Protection Board.
- The tasks of the European Data Protection Board include, for example, monitoring the correct application of the regulation, advising the Commission on relevant issues, and issuing opinions, guidelines or best practices on a variety of topics.
- The main difference is that the European Data Protection Board will not only issue opinions, as under Directive 95/46/EC. It will also issue binding decisions regarding cases where a supervisory authority has raised a relevant and reasoned objection in cases of one-stop-shops; where there are conflicting views on which of the supervisory authorities is the lead; and, finally, where the competent supervisory authority does not request or does not follow the opinion of the EDPB. The objective is to ensure a consistent application of the regulation throughout the Member States.

Independent supervision is an essential component of European data protection law. Both EU and CoE law view the existence of independent supervisory authorities as indispensable for the effective protection of the individuals' rights and freedoms regarding the processing of their personal data. As data processing is now ever-present and increasingly complex for individuals to understand, these authorities are the watchdogs of the digital age. In the EU, the existence of independent supervisory authorities is considered one of the most essential elements of the right to the protection of personal data, enshrined in primary EU law. Article 8 (3) of the EU Charter of Fundamental Rights and Article 16 (2) of the TFEU recognise the protection of personal data as a fundamental right and affirm that compliance with data protection rules must be subject to control by an independent authority.

The importance of independent supervision for data protection law has also been acknowledged in case law.

Example: In *Schrems*,[491] the CJEU was concerned with whether or not the forwarding of personal data to the United States (US) under the first EU-US Safe Harbour Agreement was in accordance with EU data protection law, in light of Edward Snowden's revelations on the US National Security Agency's conduct of mass surveillance. The transfer of personal data to the US was based on a European Commission decision adopted in 2000, which allowed personal data to be transferred from the EU to US organisations that

491 CJEU, C-362/14, *Maximilliam Schrems v. Data Protection Commissioner* [GC], 6 October 2015.

self-certify under the Safe Harbour scheme, on the basis that the scheme ensures an adequate level of protection of personal data. When requested to investigate the applicant's complaint as to the legality of data transfers after the Snowden revelations, the Irish supervisory authority rejected the complaint on the ground that the existence of the Commission decision on the adequacy of the US data protection regime reflected in the Safe Harbour principles (the 'Safe Harbour Decision'), prevented it from further investigating the complaint.

The CJEU, however, held that the existence of a Commission decision allowing data transfers to third countries that ensure adequate levels of protection does not eliminate or reduce the powers of national supervisory authorities. The CJEU noted that the powers of these authorities to monitor and ensure compliance with EU rules on data protection derive from the primary law of the EU, in particular Article 8 (3) of the Charter and Article 16 (2) of the TFEU. "The establishment of independent supervisory authorities is therefore [...] an essential component of the protection of individuals with regard to the processing of personal data."[492]

The CJEU therefore decided that even where the transfer of personal data has been subject to a Commission adequacy decision, where a complaint is lodged with a national supervisory authority, the authority must examine the complaint with diligence. The supervisory authority may reject the complaint if it finds that it is unfounded. In such a case, the CJEU emphasised that the right to an effective judicial remedy requires that individuals must be able to challenge such a decision before the national courts, who may refer the matter to the CJEU for a preliminary ruling on the validity of the Commission decision. Where the supervisory authority considers the complaint well-founded, it must be able to engage in legal proceedings and bring the matter before the national courts. The national courts may refer the case to the CJEU, as it is the only body with the power to decide the validity of a Commission adequacy decision.[493]

The CJEU then examined the validity of the Safe Harbour Decision to establish whether or not the transfers system was in accordance with EU data protection rules. It found that Article 3 of the Safe Harbour Decision

492 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 6 October 2015, para. 41.

493 *Ibid*., paras. 53–66.

restricted the powers of national supervisory authorities (granted under the Data Protection Directive) to take action to prevent data transfers in the event of an inadequate level of protection of personal data in the US. In view of the importance of independent supervisory authorities in ensuring compliance with data protection law, the CJEU held that, under the Data Protection Directive and read in light of the Charter, the Commission did not have the power to restrict the powers of the independent supervisory authorities in that way. The limitation of the powers of the supervisory authorities was one of the reasons the CJEU declared the Safe Harbour Decision invalid.

European law thus requires independent supervision as an important mechanism to ensure effective data protection. Independent supervisory authorities are the first contact point for data subjects in cases of privacy breaches.[494] Under EU law and CoE law, the establishment of supervisory authorities is mandatory. Both legal frameworks describe the tasks and powers of these authorities in a similar manner to those included in the GDPR. In principle, supervisory authorities should, therefore, function in the same manner under EU law and CoE law.[495]

5.1. Independence

EU law and **CoE law** require each supervisory authority to act with complete independence in performing its tasks and when exercising its powers.[496] The independence of the supervisory authority and its members, as well as of staff from direct or indirect external influences, is fundamental in guaranteeing full objectivity when deciding on data protection matters. Not only must the law underpinning a supervisory body's creation contain provisions specifically guaranteeing independence, but the organisational structure of the authority must demonstrate independence. In 2010, the CJEU – for the first time – examined the extent to which data protection supervisory authorities are required to be independent.[497] The highlighted examples illustrate the CJEU's definition of the meaning of 'complete independence'.

494 General Data Protection Regulation, Art. 13 (2) (d).

495 *Ibid.*, Art. 51; Modernised Convention 108, Art. 12 bis.

496 General Data Protection Regulation, Art. 52 (1); Modernised Convention 108, Art. 15 (5).

497 FRA (2010), *Fundamental rights: challenges and achievements in 2010*, Annual report 2010, p. 59; FRA (2010), *Data protection in the European Union: the role of National Data Protection Authorities*, May 2010.

Example: In *European Commission v. Federal Republic of Germany*,[498] the European Commission requested the CJEU to declare that Germany had incorrectly transposed the requirement of 'complete independence' of the supervisory authorities responsible for ensuring data protection and had thus failed to fulfil its obligations under Article 28 (1) of the Data Protection Directive. In the Commission's view, the fact that Germany had put the supervisory authorities monitoring personal data processing in the different federal states (*Länder*) under state monitoring to ensure compliance with data protection law violated the independence requirement.

The CJEU underlined that the words 'with complete independence' must be interpreted based on the actual wording of that provision and on the aims and scheme of EU Data Protection law.[499] The CJEU stressed that the supervisory authorities are 'the guardians' of rights related to personal data processing. Thus, their establishment in Member States is considered "as an essential component of the protection of individuals with regard to the processing of personal data".[500] The CJEU concluded that "when carrying out their duties, the supervisory authorities must act objectively and impartially. For that purpose, they must remain free from any external influence, including the direct or indirect influence by public authorities".[501]

The CJEU also held that the meaning of 'complete independence' should be interpreted in light of the independence of the EDPS as defined in the EU Institutions Data Protection Regulation. In this regulation, the concept of independence requires that the EDPS may neither seek nor take instructions from anybody.

Accordingly, the CJEU held that supervisory authorities in Germany – due to the oversight of public authorities – were not completely independent within the meaning of EU data protection law.

Example: In *European Commission v. Republic of Austria*,[502] the CJEU highlighted similar problems with the independence of certain members and

498 CJEU, C-518/07, *European Commission v. Federal Republic of Germany* [GC], 9 March 2010, para. 27.

499 *Ibid.*, paras. 17 and 29.

500 *Ibid.*, para. 23.

501 *Ibid.*, para. 25.

502 CJEU, C-614/10, *European Commission v. Republic of Austria* [GC], 16 October 2012, paras. 59 and 63.

staff of the Austrian Data Protection Authority (Data Protection Commission, DSK). The CJEU concluded that the fact that the Federal Chancellery supplied the supervisory authority with the workforce undermined the independence requirement set out in the EU Data Protection law. The CJEU also held that the requirement to inform the Chancellery at all times about its work negated the full independence of the supervisory authority.

Example: In *European Commission v. Hungary*,[503] similar national practices affecting the independence of the workforce were prohibited. The CJEU pointed out that "the requirement [...] to ensure that each supervisory authority is able to carry out the tasks entrusted to it in complete independence entails an obligation for the Member State concerned to allow that authority to serve its full term of office". The CJEU also held that "by prematurely bringing to an end the term served by the supervisory authority for the protection of personal data, Hungary has failed to fulfil its obligations under Directive 95/46/EC [...]."

The notion and criteria of 'complete independence' are now explicitly provided in the GDPR, which incorporates the principles established through the described CJEU judgments. Pursuant to the regulation, complete independence in performing their tasks and exercising their powers entails that:[504]

- the members of each supervisory authority must remain free from external influence – direct or indirect – and must not take instructions from anybody;
- the members of each supervisory authority must refrain from any action incompatible with their duties, to prevent conflicts of interest;
- Member States must provide each supervisory authority with the necessary human, technical and financial resources and infrastructure for the effective performance of their tasks;
- Member States must ensure that each supervisory authority chooses its own staff;

503 CJEU, C-288/12, *European Commission v. Hungary* [GC], 8 April 2014, paras. 50 and 67.

504 General Data Protection Regulation, Art. 69.

- the financial control to which each supervisory authority is subject pursuant to national law must not affect its independence. Supervisory authorities must have separate and public annual budgets which enable them to function properly.

The independence of supervisory authorities is also considered an essential requirement under CoE law. Modernised Convention 108 requires supervisory authorities to "act with complete independence and impartiality in performing their tasks and exercising their powers", without seeking or accepting instructions.[505] In this way, the convention acknowledges that these authorities cannot effectively safeguard the rights and freedoms of individuals related to data processing unless they exercise their functions with complete independence. The Explanatory Report of Modernised Convention 108 sets out a number of elements which contribute to safeguarding this independence. Such elements include the possibility for supervisory authorities to hire their own staff and to adopt decisions without being subject to external interference, as well as factors relating to the duration of the exercise of their functions and the conditions under which they may cease their functions.[506]

5.2. Competence and powers

Under EU law, the GDPR outlines the competences and organisational structure of supervisory authorities and mandates that they must be competent and have the power to perform the tasks required under the regulation.

The supervisory authority is the main body in national law that ensures compliance with EU Data Protection law. Supervisory authorities have a comprehensive catalogue of tasks and powers beyond monitoring, which include proactive and preventive supervision activities. To carry out these tasks, supervisory authorities must have appropriate investigative, corrective and advisory powers as enumerated in Article 58 of the GDPR, such as to:[507]

- advise controllers and data subjects on all matters of data protection;
- authorise standard contract clauses, binding corporate rules or administrative arrangements;
- investigate processing operations and intervene accordingly;

505 Modernised Convention 108, Art. 15 (5).

506 Explanatory Report of Modernised Convention 108.

507 General Data Protection Regulation, Art. 58. See also Convention 108, Additional Protocol, Art. 1.

- require the submission of any information relevant for the supervision of controller activities;
- warn or reprimand controllers and order notifications of personal data breaches to be sent to data subjects;
- order the rectification, blocking, erasure or destruction of data;
- impose a temporary or definitive ban on processing or impose administrative fines;
- refer a matter to court.

To exercise its functions, a supervisory authority must have access to all personal data and information necessary for an enquiry, as well as access to any premises in which a controller keeps relevant information. According to the CJEU, the powers of the supervisory authority must be interpreted broadly to ensure full effectiveness of data protection for data subjects in the EU.

> Example: In *Schrems*, the CJEU was concerned with whether the transfer of personal data to the US under the first EU-US Safe Harbour Agreement was in accordance with EU data protection law, in light of the revelations made by Edward Snowden. The CJEU's reasoning held that national supervisory authorities – acting in their capacity as independent monitors of data processing by controllers – can prevent personal data from being transferred to a third country despite the existence of an adequacy decision if there is reasonable evidence that the adequate protection is no longer guaranteed in the third country.[508]

Each supervisory authority is competent to exercise investigative powers and powers of intervention within its territory. However, as controllers' and processors' activities are often cross-border and data processing affects data subjects located in multiple Member States, the question arises concerning the division of competences between the different supervisory authorities. The CJEU had the opportunity to examine this issue in the *Weltimmo* case.

508 CJEU, C-362/14, *Maximilian Schrems v. Data Protection Commissioner* [GC], 6 October 2015, paras. 26–36 and 40–41.

Example: In *Weltimmo,*[509] the CJEU was concerned with the competence of national supervisory authorities to deal with matters involving organisations not established in their jurisdiction. Weltimmo was a company registered in Slovakia, running a property dealing website for Hungarian properties. Advertisers lodged a complaint with the Hungarian data protection supervisory authority for infringement of Hungarian data protection law, and the authority fined Weltimmo. The company challenged the fine before the national courts, and the case was referred to the CJEU to establish whether the EU Data Protection Directive allowed the supervisory authorities of a Member State to apply its national data protection law to a company registered in another Member State.

The CJEU interpreted Article 4 (1) (a) of the Data Protection Directive as permitting the application of data protection law of a Member State other than the Member State in which the controller is registered, "insofar as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity – even a minimal one – in the context of which that processing is carried out". The CJEU observed that, based on the information before it, Weltimmo pursued a real and effective activity in Hungary, as the company had a representative in Hungary included in the Slovak companies register with a Hungarian address, as well as a Hungarian bank account and letter box, and also pursued activities in Hungary written in Hungarian. This information indicated the existence of an establishment, and would make Weltimmo's activity subject to Hungarian data protection law and the jurisdiction of the Hungarian supervisory authority. However, the CJEU left it to the national court to verify the information and decide if in fact Weltimmo had an establishment in Hungary.

If the referring court found that Weltimmo had an establishment in Hungary, the Hungarian supervisory authority would have the power to impose a fine. Nevertheless, if the national court decided the contrary, i.e. that Weltimmo did not have an establishment in Hungary, the applicable law would consequently be that of the Member State(s) in which the company was registered. In this case, since the powers of supervisory authorities must be exercised in compliance with the territorial sovereignty of other Member States, the Hungarian authority would not be able to impose penalties. As

509 CJEU, C-230/14, *Weltimmo s.r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 October 2015.

the Data Protection Directive included a duty of cooperation for supervisory authorities, the Hungarian authority could, however, request its Slovak counterpart to examine the matter, establish an infringement of Slovak law, and impose the penalties provided under the Slovak legislation.

With the adoption of the GDPR, detailed rules are now in place regarding the competence of supervisory authorities in cross-border cases. The regulation establishes a 'one-stop-shop mechanism' and includes provisions mandating cooperation between different supervisory authorities. For effective cooperation in cross-border cases, the GDPR requires a lead supervisory authority to be established as the supervisory authority of the controller's or processor's main establishment or single establishment.[510] The lead supervisory authority is in charge of cross-border cases, is the controller's or processor's sole interlocutor and coordinates cooperation with other supervisory authorities to reach consensus. The cooperation includes exchanging information, mutually assisting with monitoring and investigating and adopting binding decisions.[511]

In CoE law, the supervisory authorities' competences and powers are provided in Article 15 of Modernised Convention 108. These powers correspond to those given to supervisory authorities under EU law, including powers of investigation and intervention, powers to issue decisions and impose administrative sanctions regarding violations of the provisions of the convention, and powers to engage in legal proceedings. Independent supervisory authorities also have the competence to deal with requests and complaints lodged by data subjects, to raise public awareness of data protection law and to provide advice to national decision makers for any legislative or administrative measures which provide for personal data processing.

5.3. Cooperation

The GDPR establishes a general framework for cooperation between supervisory authorities and provides more specific rules on the cooperation of supervisory authorities in cross-border activities of data processing.

Under the GDPR supervisory authorities shall provide mutual assistance and share relevant information to implement and apply the regulation in a consistent

510 General Data Protection Regulation, Art. 56 (1).

511 *Ibid.,* Art. 60.

manner.[512] This includes the requested supervisory authority carrying out consultations, inspections and investigations. Supervisory authorities can carry out joint operations, including joint investigations and joint enforcement measures whereby staff of all supervisory authorities are involved.[513]

In the EU, controllers and processors increasingly operate at a transnational level. This requires close cooperation between the competent supervisory authorities in Member States to ensure that personal data processing complies with the requirements of the GDPR. Under the regulation's 'one-stop-shop' mechanism, if a controller or processor has establishments in several Member States, or if it has a single establishment but the processing operations substantially affect data subjects in more than one Member State, the supervisory authority of the main (or single) establishment is the lead authority for controller's or processor's cross-border activities. Lead authorities have the power to take enforcement action against the controller or processor. The one-stop-shop mechanism aims to improve harmonisation and the uniform application of EU data protection law across different Member States. It is also beneficial for businesses, as they only need to deal with the lead authority rather than with several supervisory authorities. This enhances legal certainty for businesses and, in practice, should also mean that decisions are taken faster and that businesses are not faced with different supervisory authorities imposing conflicting requirements on them.

Identifying the lead authority entails determining the location of the main establishment of a business in the EU. The term 'main establishment' is defined in the GDPR. In addition, the Article 29 Working Party has issued guidelines for identifying a controller or processor's lead supervisory authority, which include the criteria for identifying the main establishment.[514]

To ensure a high level of data protection throughout the EU, the lead supervisory authority does not act alone. It must cooperate with the other supervisory authorities concerned to adopt decisions on personal data processing by controllers and processors, in an endeavour to reach consensus and ensure consistency. Cooperation among the relevant supervisory authorities includes exchanging information, mutually assisting each other, conducting joint investigations and monitoring activities.[515] When providing mutual assistance to each other, supervisory authorities

512 *Ibid.*, Art. 61 (1)–(3) and 62 (1).

513 *Ibid.*, Art. 62 (1).

514 Article 29 Working Party (2016), *Guidelines for identifying a controller or processor's lead supervisory authority*, WP 244, Brussels, 13 December 2016, revised on 5 April 2017.

515 General Data Protection Regulation, Art. 60 (1)–(3).

must accurately deal with information requests made by other supervisory authorities and exercise supervisory measures, such as, for example, prior authorisations and consultations with the data controller on its processing activities, inspections or investigations. Mutual assistance to supervisory authorities in other Member States must be provided on request without undue delay and no later than one month after receiving the request.[516]

Where the controller has establishments in multiple Member States, the supervisory authorities can conduct joint operations including investigations and enforcement measures in which staff members of the supervisory authorities of other Member States are involved.[517]

Cooperation between different supervisory authorities is an important requirement under CoE law as well. Modernised Convention 108 provides that supervisory authorities must cooperate with one another to the extent necessary to perform their tasks.[518] This should be done, for instance, by providing each other with any relevant and useful information and by coordinating investigations and conducting joint actions.[519]

5.4. The European Data Protection Board

The importance of independent supervisory authorities and the main competences they enjoy under European data protection law have been previously described in this chapter. The European Data Protection Board (EDPB) is another important actor in ensuring that data protection rules are applied effectively and consistently throughout the EU.

The GDPR established the EDPB as an EU body with legal personality.[520] It is the successor to the Article 29 Working Party,[521] which the Data Protection Directive established to advise the Commission on any EU measures affecting the rights of

516 *Ibid.*, Art. 61 (1) and (2).

517 *Ibid.*, Art. 62 (1).

518 Modernised Convention 108, Art. 16 and 17.

519 *Ibid.*, Art. 12 bis (7).

520 General Data Protection Regulation, Art. 68.

521 Under Directive 95/46/EC, Article 29 Working Party was to advise the Commission on any EU measures affecting the rights of individuals with regard to the processing of personal data and privacy, to promote the uniform application of the Directive, and to provide expert opinion to the Commission on data protection related matters. The Article 29 Working Party consisted of representatives of EU Member State supervisory authorities, together with the Commission and the EDPS.

individuals regarding personal data processing and privacy, to promote the uniform application of the directive, and to provide expert opinion to the Commission on data protection related matters. The Article 29 Working Party consisted of representatives of EU Member State supervisory authorities, together with representatives from the Commission and the EDPS.

Similar to the Working Party, the EDPB comprises the heads of the supervisory authorities of each Member State and the EDPS, or their representatives.[522] The EDPS enjoys equal voting rights, with the exception of cases related to dispute resolution, where it may vote only on decisions concerning principles and rules applicable to EU institutions which correspond in substance with those of the GDPR. The Commission has the right to participate in the EDPB's activities and meetings, but does not have voting rights.[523] The Board elects a Chair (who is entrusted with its representation) and two Deputy Chairs from among its members by simple majority for a five-year term. Furthermore, the EDPB also has a secretariat at its disposal, which the EDPS provides so that the Board has analytical, administrative and logistical support.[524]

The EDPB's tasks are detailed in Articles 64, 65 and 70 of the GDPR and include comprehensive duties which can be dived into three main activities:

- **Consistency:** The EDPB can issue legally binding decisions in three cases: where a supervisory authority has raised a relevant and reasoned objection in cases of one-stop-shops, where there are conflicting views on which of the supervisory authorities is the 'lead' and, finally, where the competent supervisory authority does not request or does not follow the EDPB's opinion.[525] The EDPB's main responsibility is to ensure that the GDPR is consistently applied throughout the EU and it plays a key role in the consistency mechanism, as described in Section 5.5.

- **Consultation:** EDPB tasks include advising the Commission on any issue related to protecting personal data in the Union, such as GDPR amendments, revisions to EU legislation which involve data processing and could be in conflict with EU data protection rules or the issuing of Commission adequacy decisions which enable the transfer of personal data to a third country or international organisation.

522 General Data Protection Regulation, Art. 68 (3).

523 *Ibid.*, Art. 68 (4) and (5).

524 *Ibid.*, Art. 73 and 75.

525 *Ibid.*, Art. 65.

- **Guidance:** The Board also issues guidelines, recommendations and best practice to encourage the consistent application of the regulation, and promotes cooperation and knowledge exchanges between supervisory authorities. In addition, it must encourage associations of controllers or processors to draw up codes of conduct, as well as to establish data protection certification mechanisms and seals.

EDPB decisions may be challenged before the CJEU.

5.5. The GDPR Consistency Mechanism

The GDPR establishes a consistency mechanism to ensure the regulation is consistently applied throughout the Member States, whereby the supervisory authorities cooperate with each other and, where relevant, with the Commission. The consistency mechanism is used in two situations. The first concerns EDPB opinions in cases where a competent supervisory authority intends to adopt measures, such as a list of processing operations requiring a Data Protection Impact Assessment (DPIA), or to determine standard contractual clauses. The second concerns EDPB binding decisions for supervising authorities in one-stop-shop cases and where a supervising authority does not follow or does not request an opinion from the EDPB.

6

Data subjects' rights and their enforcement

EU	Issues covered	CoE
Right to be informed		
General Data Protection Regulation, Article 12 CJEU, C-473/12, *Institut professionnel des agents immobiliers (IPI) v. Englebert*, 2013 CJEU, C-201/14, *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others*, 2015	Transparency of information	Modernised Convention 108, Article 8
General Data Protection Regulation, Article 13 (1) and (2) and Article 14 (1) and (2)	Content of information	Modernised Convention 108, Article 8 (1)
General Data Protection Regulation, Article 13 (1) and Article 14 (3)	Time of providing information	Modernised Convention 108, Article 9 (1) (b).
General Data Protection Regulation, Article 12 (1), (5) and (7)	Means of providing information	Modernised Convention 108, Article 9 (1) (b).
General Data Protection Regulation, Article 13 (2) (d) and Article 14 (2) (e), Articles 77, 78 and 79	Right to lodge a complaint	Modernised Convention 108, Article 9 (1) (f)
Right of access		
General Data Protection Regulation, Article 15 (1) CJEU, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*, 2009	Right of access to one's own data	Modernised Convention 108, Article 9 (1) (b) ECtHR, *Leander v. Sweden*, No. 9248/81, 1987

EU	Issues covered	CoE
CJEU, Joined cases C-141/12 and C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel* and *Minister voor Immigratie, Integratie en Asiel v. M and S*, 2014 CJEU, C-434/16, *Peter Nowak v. Data Protection Commissioner*, 2017		
Right to rectification		
General Data Protection Regulation, Article 16	Rectification of inaccurate personal data	Modernised Convention 108, Article 9 (1) (e) ECtHR, *Cemalettin Canli v. Turkey*, No. 22427/04, 2008 ECtHR, *Ciubotaru v. Moldova*, No. 27138/04, 2010
Right to erasure		
General Data Protection Regulation, Article 17 (1)	The erasure of personal data	Modernised Convention 108, Article 9 (1) (e) ECtHR, *Segerstedt-Wiberg and Others v. Sweden*, No. 62332/00, 2006
CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 2017	The right to be forgotten	
Right to restriction of processing		
General Data Protection Regulation, Article 18 (1)	Right to restrict use of personal data	
General Data Protection Regulation, Article 19	Notification obligation	
Right to data portability		
General Data Protection Regulation, Article 20	Right to data portability	
Right to object		
General Data Protection Regulation, Article 21 (1) CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 2017	Right to object due to the data subject's particular situation	Profiling Recommendation, Article 5.3 Modernised Convention 108, Article 9 (1) (d)

EU	Issues covered	CoE
General Data Protection Regulation, Article 21 (2)	Right to object to use of data for marketing purposes	Direct Marketing Recommendation, Article 4.1
General Data Protection Regulation, Article 21 (5)	Right to object by automated means	
Rights related to automated decision-making and profiling		
General Data Protection Regulation, Article 22	Rights related to automated decision-making and profiling	Modernised Convention 108, Article 9 (1) (a)
General Data Protection Regulation, Article 21	Rights to object automated decision-making	
General Data Protection Regulation, Article 13 (2) (f)	Rights to a meaningful explanation	Modernised Convention 108, Article 9 (1) (c)
Remedies, liability, sanctions and compensation		
The Charter, Article 47 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 2015 General Data Protection Regulation, Articles 77–84	For infringements of national data protection law	ECHR, Article 13 (only for CoE Member States) Modernised Convention 108, Articles 9 (1) (f), 12, 15, 16-21 ECtHR, *K.U. v. Finland*, No. 2872/02, 2008 ECtHR, *Biriuk v. Lithuania*, No. 23373/03, 2008
EU Institutions Data Protection Regulation, Articles 34 and 49 CJEU, C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd* [GC], 2010	For infringements of EU law by EU institutions and bodies	

The effectiveness of legal rules in general, and data subjects' rights in particular, depends to a considerable extent on the existence of appropriate mechanisms to enforce them. In the digital age, data processing has become ubiquitous and increasingly difficult for individuals to understand. To mitigate power imbalances between data subjects and controllers, individuals have been given certain rights to exercise greater control over the processing of their personal information. The right to access to one's own data and the right to have it rectified are enshrined in

Article 8 (2) of the EU Charter of Fundamental Rights, a document which constitutes primary EU law and has fundamental value in the EU legal order. EU secondary law – in particular the General Data Protection Regulation – has established a coherent legal framework which empowers data subjects by providing them with rights regarding data controllers. In addition to the rights of access and rectification, the GDPR recognises a series of other rights, such as the right to erasure ('right to be forgotten'), the right to object or to restrict data processing, and rights related to automated decision-making and profiling. Similar safeguards to enable data subjects to exercise effective control over their data are also included in Modernised Convention 108. Article 9 lists the rights that individuals should be able to exercise regarding the processing of their personal data. Contracting Parties must ensure that these rights are available to every data subject within their jurisdiction, and are accompanied by effective legal and practical means for enabling data subjects to exercise them.

In addition to providing individuals with rights, it is equally important to establish mechanisms that enable data subjects to challenge violations of their rights, hold controllers responsible and claim compensation. The right to an effective remedy, as guaranteed under the ECHR and the Charter, requires that judicial remedies are made available to every person.

6.1. The rights of data subjects

Key points

- Every data subject has the right to information about any data controller's processing of his or her personal data, subject to limited exemptions.
- Data subjects shall have the right to:
  - access their own data and obtain certain information about the processing;
  - have their data rectified by the controller processing their data, if the data are inaccurate;
  - have the controller erase their data, as appropriate, if the controller is processing their data illegally;
  - have the right to temporarily restrict processing;

  - have their data ported to another controller under certain conditions.
- Additionally, data subjects shall have the right to object to processing on:
  - grounds relating to their particular situation;
  - the use of their data for direct marketing purposes.
- Data subjects have the right not to be subject to decisions based solely on automated processing, including profiling, that have legal effects or that significantly affect him or her. Data subjects also have the right to:
  - obtain human intervention on the part of the controller;
  - express their point of view and contest a decision based on automated processing.

6.1.1. Right to be informed

According to **CoE law** as well as **EU law**, controllers of processing operations are obliged to inform the data subject at the time when personal data are collected about their intended processing. This obligation does not depend on a request from the data subject, rather the controller must proactively comply with the obligation, regardless of whether the data subject shows interest in the information or not.

Under CoE law, pursuant to Article 8 of Modernised Convention 108, Contracting Parties must provide that controllers inform the data subjects about their identity and habitual residence, the legal basis and purpose of the processing, the categories of personal data processed, the recipients of their personal data (if any) and how they can exercise their rights under Article 9, which includes the rights to access, rectification and legal remedy. Any other additional information deemed necessary to ensure fair and transparent personal data processing should also be communicated to the data subjects. The Explanatory Report of Modernised Convention 108 clarifies that the information presented to the data subjects "should be easily accessible, legible, understandable and adapted to the relevant data subjects".[526]

Under EU law, the transparency principle requires that any personal data processing should generally be transparent to individuals. Individuals have the right to know how and which personal data are collected, used or otherwise processed, as well as to be made aware of the risks, safeguards and their rights regarding processing.[527]

526 Explanatory Report of Modernised Convention 108, para. 68.

527 General Data Protection Regulation, Recital 39.

Article 12 of the GDPR thus establishes a broad comprehensive obligation for controllers in providing transparent information and/or communicating how data subjects can exercise their rights.[528] The information must be concise, transparent, intelligible and easily accessible, using clear and plain language. It must be provided in written form, including electronically where appropriate, and it may even be provided orally at the data subject's request and if his or her identity is proven beyond doubt. The information shall be provided without excessive delay or expense.[529]

Article 13 and Article 14 of the GDPR deal with the right of data subjects to be informed, either in situations where personal data were collected directly from them, or in situations where the data were not obtained from them, respectively.

The scope of the right to information and its limitations under EU law have been clarified in CJEU case law.

Example: In *Institut professionnel des agents immobiliers (IPI) v. Englebert*,[530] the CJEU was asked to interpret Article 13 (1) of Directive 95/46. This article gave Member States the choice of whether to adopt legislative measures to restrict the scope of the data subject's right to be informed where necessary to protect, among other things, the rights and freedoms of others and to prevent and investigate crimes or breaches of ethics for regulated professions. IPI is a professional body of real estate agents in Belgium responsible for ensuring compliance with the proper practice of the estate agent profession. It asked a national court to declare that the defendants had violated professional rules and to order them to cease various estate agency activities. The action was based on evidence provided by private detectives that IPI had used.

The national court had doubts about the value of the detectives' evidence, given the possibility that it had been obtained without respecting the data protection requirements of Belgian legislation, in particular the obligation to inform data subjects of the processing of their personal data before collecting that information. The CJEU noted that Article 13 (1) stated that Member States 'may', but have no obligation to, provide in their national law for exceptions

528 *Ibid.*, Art. 13 and 14; Modernised Convention 108, Art. 8 (1) (b).

529 General Data Protection Regulation, Art. 12 (5); Modernised Convention 108, Art. 9 (1) (b).

530 CJEU, C-473/12, *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert and Others*, 7 November 2013.

to the obligation to inform data subjects of the processing of their data. As Article 13 (1) includes the prevention, investigation, detection and prosecution of criminal offences or breaches of ethics as grounds on which Member States can limit individuals' rights, the activity of a body such as the IPI and the private detectives acting in its name could rely on that provision. However, if a Member State has not provided for such an exception, the data subjects must be informed.

Example: In *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others*,[531] the CJEU clarified whether EU law precludes a national public administrative body from transferring personal data to another public administrative body for subsequent processing, without the data subjects being informed of that transfer and of the processing. In that case, the National Administration Agency had not informed the applicants that they had transferred their data to the National Health Insurance Fund prior to the transfer.

The CJEU considered that the requirement under EU law to inform the data subject about the processing of their personal data is "all the more important since it affects the exercise by the data subjects of their right of access to, and the right to rectify, the data being processed [...] and their right to object to the processing of those data". The principle of fair processing requires informing data subjects about the transfer of their data to another public body for further processing by the latter. According to Article 13 (1) of Directive 95/46, Member States may restrict the right to be informed if it is deemed necessary to safeguard an important economic interest of the state, including taxation matters. However, such restrictions must be imposed by legislative measures. As neither the definition of the data to be transferred nor the detailed arrangements for the transferring were laid down in a legislative measure, but rather solely in a protocol between the two public authorities, the derogation conditions under EU law were not met. The applicants should have been informed in advance of the transfer of their data to the National Health Insurance Fund and the body's subsequent processing of this data.

531 CJEU, C-201/14, *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others*, 1 October 2015.

Content of the information

Under Article 8 (1) of Modernised Convention 108, the controller is obliged to provide any information to the data subject that ensures fair and transparent personal data processing, including the:

- controller's identity and habitual residence or establishment;
- legal basis and the purposes of the intended processing;
- categories of personal data processed;
- recipients or categories of recipients of the personal data, if any;
- ways in which data subjects can exercise their rights.

Under the GDPR, when personal data are collected from the data subject, the controller is obliged to provide the following information to the data subject at the time the personal data are obtained:[532]

- the controller's identity and contact details, including the DPO's details, if any;
- the purpose and legal basis for the processing, i.e. a contract or legal obligation;
- the data controller's legitimate interest, if this provides the basis for processing;
- the personal data's eventual recipients or categories of recipients;
- whether the data will be transferred to a third country or international organisation, and whether this is based on an adequacy decision or relies upon appropriate safeguards;
- the period for which the personal data will be stored, and if establishing that period is not possible, the criteria used to determine the data storage period;
- the data subjects' rights regarding processing, such as the rights of access, rectification, erasure, and to restrict or object to processing;

532 General Data Protection Regulation, Art. 13 (1); Modernised Convention 108, Art. 7 bis (1).

- whether the provision of personal data is required by law or a contract, whether the data subject is obliged to provide his or her personal data, as well as the consequences in case of failure to provide the personal data;

- the existence of automated decision-making, including profiling;

- the right to lodge a complaint with a supervisory authority;

- the existence of the right to withdraw consent.

In cases of automated decision-making, including profiling, data subjects must receive meaningful information about the logic involved in profiling, its significance and the envisaged consequences they face from the processing.

In cases where the personal data is not obtained from the data subject directly, the data controller must notify the individual about the origin of the personal data. In any case, the controller must, among other things, inform data subjects about the existence of automated decision-making, including profiling.[533] Finally, if a controller intends to process personal data for a purpose other than that originally stated to the data subject, the principles of purpose limitation and transparency require that the controller provide the data subject with information about this new purpose. Controllers must provide information prior to any further processing. In other terms, in cases where the data subject provided consent for the personal data processing, the controller must receive the data subject's renewed consent if the data processing purpose changes or if further purposes are added.

Time of providing information

The GDPR distinguishes between two scenarios and two points in time at which the data controller must provide information to the data subject:

- Where the personal data is obtained directly from the data subject, the controller must notify the data subject about all of his or her related information and rights under the GDPR at the time the data are obtained.[534]

533 General Data Protection Regulation, Art. 13 (2) and 14 (2) (f).

534 *Ibid.*, Art. 13 (1) and (2), introductory wording where the General Data Protection Regulation refers to the information on the obligation to apply at "the time when personal data are obtained".

If the controller intends to further process the personal data for a different purpose, the controller shall provide all the relevant information prior to the processing taking place.

- Where the personal data has not been obtained from the data subject directly, the controller is obliged to provide the information about the processing to the data subject "within a reasonable period after obtaining the personal data, but at the latest within one month", or before data are disclosed to a third party.[535]

The Explanatory Report of Modernised Convention 108 stipulates that if informing data subjects is not possible when commencing the processing, it can be done at a later stage, such as when the controller is put in contact with the data subject for any reason.[536]

Different ways of providing information

Under both CoE and EU law, the information the controller must provide to data subjects must be concise, transparent, intelligible and easily accessible. It must be in writing, or by other means, including electronic means, using clear, plain and easily understandable language. When providing information, the controller can use standardised icons to provide the information in an easily visible and intelligible manner.[537] For example, an icon representing a lock might be used to signal that the data is safely collected and/or encrypted. Data subjects can request to have the information provided by oral means. Information must be free of charge, unless the data subject's requests are manifestly unfounded or excessive (i.e. of a repetitive nature).[538] Easy access to the information provided is paramount to the data subject's ability to exercise his or her rights provided under EU data protection law.

The fair processing principle requires that information be easily understandable to data subjects. Language must be used which is appropriate for the addressees. The level and type of language used would need to be different depending on whether

535 *Ibid*., Art. 13 (3) and 14 (3); see also the reference to reasonable intervals and without excessive delay under the Modernised Convention 108, Art. 8 (1) (b).

536 Explanatory Report of Modernised Convention 108, para. 70.

537 The European Commission will further develop information to be presented by the icons and the procedures for providing standardised icons by means of delegated acts; see General Data Protection Regulation, Art. 12 (8).

538 General Data Protection Regulation, Art. 12 (1), (5) and (7) and Modernised Convention 108, Art. 9 (1) (b).

the intended audience is, for example, an adult or a child, the general public or an academic expert. The question of how to balance this aspect of understandable information is considered in the Article 29 Working Party Opinion on More Harmonised Information Provisions. This promotes the idea of so-called layered notices,[539] allowing the data subject to decide which level of detail he or she prefers. However, this way of presenting information does not relieve the controller from its obligation under Article 13 and Article 14 of the GDPR. The controller must still provide all information to the data subject.

One of the most efficient ways to provide information is to place appropriate information clauses on the controller's home page, such as a website privacy policy. There is, however, a significant part of the population that does not use the internet, and a company's or public authority's information policy should take this into account.

A privacy notice about personal data processing on a web page could look as follows:

Who are we?

The data processing 'controller' is Bed and Breakfast C&U, established in [Address: xxx], Tel: xxx; Fax: xxx; Email at info@c&u.com; Data Protection Officer contact details: [xxx].

The personal data information notice forms part of the terms and conditions governing our hotel services.

What data do we collect from you?

We collect the following personal data from you: your name, postal address, telephone number, email address, stay information, credit and debit card number and IP addresses or domain names of the computers you used to connect to our website.

Why are we collecting your data?

We process your data on the basis of your consent and for the purposes of carrying out reservations, for concluding and fulfilling the contracts related

539 Article 29 Working Party (2004), *Opinion 10/2004 on More Harmonised Information Provisions*, WP 100, Brussels, 25 November 2004.

to the services we offer to you and for complying with requirements imposed by law, for instance the Local Fees Act, which requires us to collect personal data to enable payment of the city tax for accommodation.

How do we process your data?

Your personal data will be retained for a period of three months. Your data are not subject to automatic decision procedures.

Our Bed and Breakfast C&U follows strict security procedures to ensure that your personal information is not damaged, destroyed, or disclosed to a third party without your permission and to prevent unauthorised access. The computers storing the information are kept in a secure environment with restricted physical access. We use secure firewalls and other measures to restrict electronic access. If the data must be transferred to a third party, we require them to have in place similar measures to protect your personal data.

All of the information we collect or record is restricted to our offices. Only persons who need the information to fulfil their duties under this contract are granted access to personal data. We will explicitly ask you when we need information to identify you. We may require you to cooperate with our security checks before we disclose information to you. You can update the personal information that you give us at any time by contacting us directly.

What are your rights?

You have the right to access your data, to obtain a copy of your data, to request their erasure or rectification, or request your data to be ported to another controller.

You may contact us at info@c&u.com with your requests. We must answer your request within one month, but if your request is too complex or we receive too many other requests we will inform you that this period may be extended by a further two months.

Accessing your personal data

You have the right to access your data, to be provided, on request, with knowledge of the reasoning underlying data processing, to request their

erasure or rectification and the right not to be subject to a purely automated decision without having your views taken into consideration. You may contact us at info@c&u.com with your requests. You also have the right to object to the processing, withdraw your consent and lodge a complaint with the national supervisory authority should you consider that this data processing is in violation of the law and to claim compensation for damage incurred as a result of the unlawful processing.

The right to lodge a complaint

The GDPR requires the controller to inform data subjects about enforcement mechanisms under national and EU law for cases of personal data breaches. The controller must inform data subjects about their right to lodge a complaint about a personal data breach with a supervisory authority and, if necessary, with a national court.[540] CoE law also prescribes the right of data subjects to be informed of the means of exercising their rights, including the right to have a remedy laid down in Article 9 (1) (f).

Exemptions from the obligation to inform

The GDPR provides exception to the obligation to inform. Under Article 13 (4) and Article 14 (5) of the GDPR, the obligation to inform data subjects does not apply if the data subject already has all of the relevant information.[541] In addition, where the personal data have not been obtained from the data subject, the obligation to inform will not apply if the provision of information is impossible or disproportionate, in particular where the personal data is processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[542]

Furthermore, Member States enjoy a margin of discretion under the GDPR to restrict obligations and rights provided to individuals under the regulation if this is a necessary and proportionate measure in a democratic society, for instance, to safeguard national and public security, defence, protection of judicial investigations and

540 General Data Protection Regulation, Art. 13 (2) (d) and 14 (2) (e); Modernised Convention 108, Art. 8 (1) (f).

541 *Ibid*., Art. 13 (4) and 14 (5) (a).

542 *Ibid*., Art. 14 (5) (b)–(e).

proceedings, or the protection of economic and financial interests, as well as private interests which are more compelling than data protection interests.[543]

Any exemptions or restrictions must be necessary in a democratic society and proportionate to the aim pursued. In very exceptional cases, for instance because of medical indications, the data subject's protection may itself require a restriction of transparency; this relates especially to restricting the right of access of every data subject.[544] As a minimum level of protection, however, national law must respect the essence of the fundamental rights and freedoms protected under EU law.[545] This requires that the national law contains specific provisions clarifying the purpose of the processing, categories of personal data included, safeguards and other procedural requirements.[546]

Where data are collected for scientific or historical research purposes, statistical purposes or for archiving purposes in the public interest, Union or Member States law can provide derogations from the obligation to inform if it is likely to render impossible or seriously impair the achievement of the specific purposes.[547]

Similar limitations exist under CoE law, where rights granted to data subjects under Article 9 of Modernised Convention 108 can be subject to possible restrictions under Article 11 of Modernised Convention 108, under strict conditions. Furthermore, according to Article 8 (2) of Modernised Convention 108 the obligation of transparency of processing imposed to controllers does not apply where the data subject already has the information.

The right of access to an individual's own data

Under CoE law, the right of access to an individual's own data is explicitly acknowledged in Article 9 of Modernised Convention 108. This provides that every individual has the right to obtain, upon request, information about the processing of personal data relating to him or her, which is communicated in an intelligible manner. The right of access has been recognised not only in the provisions of Modernised Convention 108, but also in ECtHR case law. The ECtHR has repeatedly held that individuals

543 General Data Protection Regulation, Art. 15 (4).

544 General Data Protection Regulation, Art. 15.

545 General Data Protection Regulation, Art. 23 (1).

546 *Ibid.*, Art. 23 (2).

547 *Ibid.*, Art. 89 (2) and (3).

have a right to access information about their personal data, and that this right arises from the need to respect private life.[548] However, the right to access personal data stored by public or private organisations may in certain circumstances be limited.[549]

Under EU law, the right to access one's own data is explicitly acknowledged in Article 15 of the GDPR and it is also set out as an element of the fundamental right to the protection of personal data in Article 8 (2) of the EU Charter of Fundamental Rights.[550] An individual's right to gain access to his or her own personal data is a key element of European data protection law.[551]

The GDPR provides that every data subject has the right to access his or her personal data and certain information about the processing, which the controllers must provide.[552] In particular, every data subject has a right to obtain (from the controller) confirmation as to whether or not data relating to him or her are being processed, and information about at least the following:

- processing purposes;
- categories of data concerned;
- recipients or categories of recipients to whom the data are disclosed;
- period for which the data is intended to be stored, or, if not possible, the criteria used to determine that period;
- existence of rights to rectify or to erase personal data, or to restrict personal data processing;
- right to lodge a complaint with the supervisory authority;

548 ECtHR, *Gaskin v. the United Kingdom*, No. 10454/83, 7 July 1989; ECtHR, *Odièvre v. France* [GC], No. 42326/98, 13 February 2003; ECtHR, *K.H. and Others v. Slovakia*, No. 32881/04, 28 April 2009; ECtHR, *Godelli v. Italy*, No. 33783/09, 25 September 2012.

549 ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987.

550 Also see CJEU, Joined cases C-141/12 and C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel* and *Minister voor Immigratie, Integratie en Asiel v. M and S*, 17 July 2014; CJEU, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (EFSA), European Commission*, 16 July 2015.

551 CJEU, Joined cases C-141/12 and C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel* and *Minister voor Immigratie, Integratie en Asiel v. M and S*, 17 July 2014.

552 General Data Protection Regulation, Art. 15 (1).

- any available information about the source of the data undergoing processing if the data are not collected from the data subject;

- in the case of automated decisions, the logic involved in any automated processing of data.

The data controller must provide the data subject with a copy of the personal data being processed. Any information communicated to the data subject must be provided in an intelligible form, which means that the controller must make sure the data subject can understand the information being provided. For example, including technical abbreviations, coded terms or acronyms in response to an access request will usually not suffice, unless the meaning of these terms is explained. Where automated decision-making is carried out, including profiling, the general logic involved in the automated decision-making will need to be explained, including the criteria which have been considered when evaluating the data subject. Similar requirements exist under **CoE law**.[553]

Example: Accessing his or her personal data will help a data subject to determine whether or not the data are accurate. It is, therefore, essential that the data subject is informed, in an intelligible form, not only of the actual personal data that are being processed, but also the categories under which these personal data are processed, such as name, IP address, geolocation coordinates, credit card number, etc.

Information about the source of data – when the data are not collected from the data subject – must be given in the response to an access request, as far as this information is available. This provision must be understood in the context of the principles of fairness, transparency and accountability. A controller may not destroy information about the source of data in order to be exempt from disclosing it, – unless the deletion would have taken place despite the access request having being received – and it must still comply with its general 'accountability' requirements.

As set out in CJEU case law, the right to access personal data may not be unduly restricted by time limits. Data subjects must also be given a reasonable opportunity to gain information about data processing operations that took place in the past.

553 See Modernised Convention 108, Art. 8 (1) (c).

Example: In *Rijkeboer*,[554] the CJEU was asked to determine whether an individual's right to access information about the recipients or categories of recipient of personal data, and to the content of the data, could be limited to one year before his or her request for access.

To determine whether EU legislation authorises such a time limit, the CJEU decided to interpret Article 12 in light of the purposes of the directive. The CJEU first stated that the right of access is necessary to enable the data subject to exercise the right to have the controller rectify, erase or block their data, or to notify third parties to whom the data have been disclosed of that rectification, erasure or blocking. An effective right of access is also necessary to enable the data subject to exercise their right to object to the processing of their personal data or their right to lodge a complaint and claim damages.[555]

To ensure the practical effect of the rights given to data subjects, the CJEU held that "that right must of necessity relate to the past. If that were not the case, the data subject would not be in a position effectively to exercise his right to have data presumed unlawful or incorrect rectified, erased or blocked or to bring legal proceedings and obtain compensation for the damage suffered".

6.1.2. Right to rectification

Under EU law and **CoE Law**, data subjects have the right to have their personal data rectified. The accuracy of personal data is essential to ensure a high level of data protection for data subjects.[556]

Example: In *Ciubotaru v. Moldova*,[557] the applicant was unable to change the registration of his ethnic origin in official records from Moldovan to Romanian allegedly due to the fact that he had failed to substantiate his request. The ECtHR considered it acceptable for States to require objective evidence when

554 CJEU, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*, 7 May 2009.

555 General Data Protection Regulation, Art. 15 (1) (c) and (f), 16, 17 (2) and 21, and Chapter VIII.

556 *Ibid*., Art. 16 and Recital 65; Modernised Convention 108, Art. 9 (1) (e).

557 ECtHR, *Ciubotaru v. Moldova*, No. 27138/04, 27 April 2010, paras. 51 and 59.

registering an individual's ethnic identity. When such a claim was based on purely subjective and unsubstantiated grounds, the authorities could refuse. However, the applicant's claim had been based on more than the subjective perception of his own ethnicity; he had been able to provide objectively verifiable links with the Romanian ethnic group such as language, name, empathy and others. Nonetheless, under domestic law, the applicant was required to provide evidence that his parents had belonged to the Romanian ethnic group. Given the historical realities of Moldova, such a requirement had created an insurmountable barrier to registering an ethnic identity other than the one that Soviet authorities had recorded regarding his parents. In preventing the applicant from having his claim examined in the light of objectively verifiable evidence, the State had failed to comply with its positive obligation to secure to the applicant effective respect for his private life. The Court concluded that there had been a violation of Article 8 of the ECHR.

In some cases, it will be sufficient for the data subject to simply request rectification of, for example, the spelling of a name, a change of address or a telephone number. According to **EU law** and **CoE law**, inaccurate personal data must be rectified without undue or excessive delay.[558] If, however, such requests are linked to legally significant matters, such as the data subject's legal identity, or the correct place of residence for the delivery of legal documents, requests for rectification may not be enough and the controller may be entitled to demand proof of the alleged inaccuracy. Such demands must not place an unreasonable burden of proof on the data subject and thereby preclude data subjects from having their data rectified. The ECtHR has found violations of Article 8 of the ECHR in several cases where the applicant had been unable to challenge the accuracy of information kept in secret registers.[559]

Example: In *Cemalettin Canli v. Turkey*,[560] the ECtHR found a violation of Article 8 of the ECHR in the incorrect police reporting in criminal proceedings.

The applicant had twice been involved in criminal proceedings because of alleged membership in illegal organisations but had not been convicted.

558 General Data Protection, Art. 16; Modernised Convention 108, Art. 9 (1).

559 ECtHR, *Rotaru v. Romania* [GC], No. 28341/95, 4 May 2000.

560 ECtHR, *Cemalettin Canli v. Turkey*, No. 22427/04, 18 November 2008, paras. 33 and 42–43; ECtHR, *Dalea v. France*, No. 964/07, 2 February 2010.

When the applicant was again arrested and indicted for another criminal offence, the police submitted to the criminal court a report entitled "*information form on additional offences*", in which the applicant was said to be a member of two illegal organisations. The applicant's request to have the report and the police records amended was unsuccessful. The ECtHR held that the information in the police report fell within the scope of Article 8 of the ECHR, as systematically collected public information stored in files held by the authorities could also fall within the meaning of 'private life'. Moreover, the police report was incorrect in its drafting, and its submission to the criminal court had not been in accordance with domestic law. The Court concluded that there had been a violation of Article 8.

During civil litigation or proceedings before a public authority to decide whether data are correct or not, the data subject can ask for an entry or note to be placed on his or her data file stating that the accuracy is contested and that an official decision is pending.[561] During this period, the data controller must not present the data as correct or not subject to amendment, particularly to third parties.

6.1.3. Right to erasure ('the right to be forgotten')

Providing data subjects with a right to have their own data erased is particularly important for the effective application of data protection principles, and notably the principle of data minimisation (personal data must be limited to what is necessary for the purposes for which those data are processed). A right to erasure is therefore found in both the CoE and EU legal instruments.[562]

Example: In *Segerstedt-Wiberg and Others v. Sweden*,[563] the applicants had been affiliated with certain liberal and communist political parties. They suspected that information about them had been entered into security police records and requested its erasure. The ECtHR was satisfied that the storage of the data at issue had a legal basis and pursued a legitimate aim. However, in respect of some of the applicants, the ECtHR found that the continued retention of the data was a disproportionate interference with

561 General Data Protection Regulation, Art. 16, second sentence.

562 *Ibid.*, Art. 17.

563 ECtHR, *Segerstedt-Wiberg and Others v. Sweden*, No. 62332/00, 6 June 2006, paras. 89 and 90; see also, for example, ECtHR, *M.K. v. France*, No. 19522/09, 18 April 2013.

their private lives. For example, in the case of one applicant, the authorities retained information that in 1969, he had allegedly advocated violent resistance to police control during demonstrations. The ECtHR found that this information could have no relevant national security interest, particularly given its historical nature. The Court found a violation of Article 8 of the ECHR regarding four of the five applicants as, given the lengthy time lapse since the applicants' alleged acts, the continued storage of their data lacked relevance.

Example: In *Brunet v. France*,[564] the applicants denounced the storage of their personal information in a police database which contained information on convicted persons, accused persons and victims. Even though the criminal proceedings against the applicant had been discontinued, his details appeared in the database. The ECtHR held that there had been a violation of Article 8 of the ECHR. In reaching its conclusion, the Court considered that, in practice, there was no possibility for the applicant to have his personal data deleted from the database. The ECtHR also considered the nature of the information included in the database and deemed that it was intrusive to the applicant's privacy, as it contained details of his identity and personality. In addition, it found that the retention period for personal records in the database, which amounted to 20 years, was excessively lengthy, particularly since no court had ever convicted the applicant.

Modernised Convention 108 explicitly recognises that every individual has a right to the erasure of inaccurate, false or unlawfully processed data.[565]

Under EU law, Article 17 of the GDPR gives effect to data subjects' requests to have data erased or deleted. The right to have one's personal data erased without undue delay applies where:

- the personal data are no longer necessary regarding the purposes for which they were collected or otherwise processed;
- the data subject withdraws the consent on which the processing is based and there is no other legal ground for the processing;

564 ECtHR, *Brunet v. France*, No. 21010/10, 18 September 2014.

565 Modernised Convention 108, Art. 9 (1) (e).

- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- the personal data have been collected concerning the offer of information society services to children pursuant to Article 8 of the GDPR.[566]

The burden of proof that the data processing is legitimate will fall on the data controllers, as they are responsible for the lawfulness of the processing.[567] According to the principle of accountability, the controller must at any time be able to demonstrate that there is a sound legal basis to its data processing, otherwise the processing must be stopped.[568] The GDPR defines exceptions to the right to be forgotten, including where the processing of personal data is necessary for:

- exercising the right of freedom of expression and information;
- compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- reasons of public interest in the area of public health;
- archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;
- the establishment, exercise or defence of legal claims.[569]

The CJEU has affirmed the importance of the right to erasure to ensure a high level of data protection.

566 General Data Protection Regulation, Art. 17 (1).

567 *Ibid*.

568 *Ibid*., Art. 5 (2).

569 *Ibid*., Art. 17 (3).

Example: In *Google Spain*,[570] the CJEU was concerned with whether Google was required to delete outdated information regarding financial difficulties about the applicant from its search list results. Among other things, Google contested being responsible, arguing that it merely provides a hyperlink to the publisher's web page that hosts the information, in this case a newspaper reporting on the applicant's insolvency issues.[571] Google argued that the request to delete outdated information from a web page should be made to the host of the web page and not to Google, which simply provides a link to the original page. The CJEU concluded that Google, when it searches the web for information and web pages, and when it indexes content to provide search results, becomes a data controller to which responsibilities and obligations under EU law apply.

The CJEU clarified that internet search engines and search results providing personal data can establish a detailed profile of an individual.[572] Search engines render the information contained in such a list of results ubiquitous. In light of its potential seriousness, that interference cannot be justified by merely the economic interest which the operator of such an engine has in that processing. A fair balance must be sought in particular between the legitimate interest of internet users in access to information and the data subject's fundamental rights under Articles 7 and 8 of the EU Charter of Fundamental Rights. In an increasingly digitised society, the requirement for personal data to be accurate and not go beyond what is necessary (i.e. for public information) is fundamental to ensure a high level of data protection to individuals. The "controller in respect of that processing must ensure, within the framework of its responsibilities, powers and capabilities, that that processing meets the requirements" of EU law, so that the established legal guarantees have full effect.[573] This means that the right to have one's

570 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 May 2014, paras. 55–58.

571 Google also contested the application of the EU data protection rules due to the fact that Google Inc. is established in the US and the processing of the personal data at issue in the case was also carried out in the US. A second argument for the inapplicability of EU data protection law related to the claim that search engines cannot be regarded as 'controllers' in respect of the data displayed in their results, as they have no knowledge of the data nor do they exercise control over them. The CJEU dismissed both arguments, holding that Directive 95/46/EC was applicable in that case, and continued with examining the scope of the rights it guaranteed, in particular the right to erasure of the personal data.

572 *Ibid.*, paras. 36, 38, 80–81 and 97.

573 *Ibid.*, paras. 81–83.

personal data erased when the processing is outdated or no longer necessary also covers data controllers that replicate the information.[574]

Considering whether or not Google was required to remove the links related to the applicant, the CJEU held that under certain conditions, individuals have the right to request personal data to be erased. This right may be invoked where information relating to an individual is inaccurate, inadequate, irrelevant or excessive for the data processing purposes. The CJEU acknowledged that this right is not absolute; it must be balanced with other rights and interests, in particular the interest of the general public in having access to certain information. Each request for erasure must be assessed on a case-by-case basis to strike a balance between the fundamental rights to the protection of personal data and private life of the data subject on the one hand, and the legitimate interests of all internet users, including publishers, on the other. The CJEU provided guidance on the factors to consider during this balancing exercise. The nature of the information in question is a particularly important factor. If the information relates to the private life of the individual, and there is no public interest in the availability of the information, data protection and privacy would override the right of the general public to have access to the information. On the contrary, if it appears that the data subject is a public figure, or that the information is of such a nature as to justify it being available to the general public, then the general public's preponderant interest in having access to the information may justify the interference with the data subject's fundamental rights to data protection and privacy.

Following the judgment, the Article 29 Working Party adopted guidelines for implementing the CJEU ruling.[575] The guidelines include a list of common criteria for the supervisory authorities to use when handling complaints related to individuals' requests for deletion, explaining what that right to erasure entails, and guiding them in this balancing of rights exercise. The guidelines reiterate that assessments need

574 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 May 2014, para. 88. See also Article 29 Data Protection Working Party (2014), *Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, WP 225, Brussels, 26 November 2014 and Recommendation CM/Rec 2012(3) of the Committee of Ministers to member states on the protection of human rights with regard to search engines, 4 April 2012.

575 Article 29 Working Party (2014), *Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, WP 225, Brussels, 26 November 2014.

to be made on a case-by-case basis. As the right to be forgotten is not absolute, the outcome of a request may differ depending on the case at stake. This is also illustrated in the case law of the CJEU after Google.

Example: In *Camera di Commercio di Lecce v. Manni*,[576] the CJEU had to examine whether an individual had a right to obtain the erasure of his personal data published in a Public Registry of Companies, once his company ceased to exist. Mr Manni had requested the Lecce Chamber of Commerce to delete his personal data from that registry, having discovered that potential clients would consult the registry and see that he had previously been the administrator of a company declared bankrupt more than a decade earlier. The applicant believed that this information would deter potential clients.

In balancing Mr Manni's right to the protection of his personal data with the general public's interest in access to the information, the CJEU first examined the purpose of the public registry. It pointed to the fact that disclosure was provided for by law, and in particular by an EU directive aiming to make company information more easily accessible to third parties. Third parties should thus have access and be able to examine the basic documents of a company and other information concerning the company, "especially particulars of the persons who are authorised to bind the company". The purpose of the disclosure was also to guarantee legal certainty in view of intensified trade between Member States, by ensuring that third parties have access to all of the relevant information about companies across the EU.

The CJEU further noted that even after the passage of time, and even after a company is dissolved, rights and legal obligations related to the company often continue to exist. Disputes related to dissolution may be lengthy, and questions concerning a company, its managers and liquidators may arise for many years after a company has ceased to exist. The CJEU held that, in view of the range of possible scenarios and the differences in the limitation periods provided in each Member States, "it seems impossible, at present, to identify a single time limit, as from the dissolution of a company, at the end of which the inclusion of such data in the register and their disclosure would no longer be necessary". Due to the legitimate aim of the disclosure and the difficulties in establishing a period at the end of which the personal

576 CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 9 March 2017.

data could be deleted from the registry without harming the interests of third parties, the CJEU found that EU data protection rules do not guarantee a right to erasure of personal data for persons in Mr Manni's situation.

Where the controller has made personal data public and is required to delete the information, the data controller is obliged and must take 'reasonable' steps to inform other controllers who process the same data, about the data subject's request for erasure. The controller's activities must take into account available technologies and the cost of implementation.[577]

6.1.4. Right to restriction of processing

Article 18 of the GDPR empowers data subjects to temporarily restrict a controller from processing their personal data. Data subjects can request the controller to restrict processing where:

- the accuracy of the personal data is contested;
- the processing is unlawful and the data subject requests that the use of the personal data be restricted instead of erased;
- the data must be kept for the exercise or defence of legal claims;
- a decision is pending on the legitimate interests of the data controller prevailing over the interests of the data subject.[578]

The methods in which a controller can restrict personal data processing can include, for example, temporary movement of the selected data to another processing system, making the data unavailable to users or the removal of personal data on a temporary basis.[579] The controller must notify the data subject before the restriction on processing is lifted.[580]

577 General Data Protection Regulation, Art. 17 (2) and Recital 66.

578 *Ibid*., Art. 18 (1).

579 *Ibid*., Recital 67.

580 *Ibid*., Art. 18 (3).

Obligation to notify regarding the rectification or erasure of personal data or processing restriction

The controller must communicate any rectification or erasure of personal data or any processing restriction to each recipient to whom the controller disclosed the personal data, insofar as this is neither impossible nor disproportionate.[581] If the data subject requests information about those recipients the controller must provide him or her with this information.[582]

6.1.5. Right to data portability

Under the GDPR, data subjects enjoy the right to data portability in situations where the personal data that they have provided to a controller are processed by automated means on the basis of consent, or where the personal data processing is necessary for the performance of a contract and is carried out by automated means. This means that the right to data portability does not apply in situations where the personal data processing is based on a legal ground other than consent or a contract.[583]

If the right to data portability is applicable, data subjects are entitled to have their personal data transmitted directly from one controller to another if this is technically feasible.[584] To facilitate this, the controller should develop interoperable formats that enable data portability for data subjects.[585] The GDPR specifies that these formats must be structured, commonly used and machine-readable to facilitate interoperability.[586] Interoperability can be defined in a broad sense as the information systems' ability to exchange data and to enable information sharing.[587] While the purpose of the formats used is to achieve interoperability, the GDPR does not impose particular recommendations on the specific format to be provided: formats may differ across sectors.[588]

581 Ad hoc Committee on Data Protection (CAHDATA), Explanatory Report of the Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, para. 79.

582 General Data Protection Regulation, Art. 19.

583 *Ibid.*, Recital 68 and Art. 20 (1).

584 *Ibid.*, Art. 20 (2).

585 *Ibid.*, Recital 68 and Art. 20 (1).

586 *Ibid.*, Recital 68.

587 European Commission, Communication on stronger and smarter information systems for borders and security, COM(2016) 205 final, 2 April 2016.

588 Article 29 Working Party (2016), *Guidelines on the right to data portability*, WP 242, 13 December 2016 and revised on 5 April 2017, p. 13.

According to the Article 29 Working Party guidelines, the right to data portability "supports user choice, user control and user empowerment", aiming to give data subjects control over their own personal data.[589] The guidelines clarify the main elements of data portability, which include:

- the data subjects' right to receive their own personal data processed by the controller in a structured, commonly used, machine-readable and interoperable format;
- the right to transmit personal data from one data controller to another data controller without hindrance if this is technically feasible;
- the regime of controllership – when a controller responds to a data portability request, they act on the data subject's instructions, meaning that they are not responsible for the recipient's compliance with data protection law, given that the data subject decides who the data is ported to;
- the exercise of the right to data portability is without prejudice to any other right as is the case with any other rights in the GDPR.

6.1.6. Right to object

Data subjects can invoke their right to object to personal data processing on grounds relating to their particular situation and to data processed for direct marketing purposes. The right to object can be exercised by automated means.

The right to object on grounds related to the data subjects' particular situations

Data subjects do not have a general right to object to the processing of their data.[590] Article 21 (1) of the GDPR empowers the data subject to raise objections on grounds relating to their particular situation where the legal basis for the processing is the controller's performance of a task carried out in the public interest, or where the processing is based on the controller's legitimate interests.[591] The right to object

589 *Ibid.*

590 See also ECtHR, *M.S. v. Sweden*, No. 20837/92, 27 August 1997 (where medical data were communicated without consent or the possibility to object); ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987; ECtHR, *Mosley v. the United Kingdom*, No. 48009/08, 10 May 2011.

591 General Data Protection Regulation, Recital 69; Art. 6 (1) (e) and (f).

applies to profiling activities. A similar right has been recognised in Modernised Convention 108.[592]

The right to object on grounds relating to the data subject's particular situation aims to strike the correct balance between the data subject's data protection rights and the legitimate rights of others in processing their data. The CJEU, however, has clarified that the data subject's rights override 'as a general rule' the economic interests of a data controller depending on "the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information".[593] Under the GDPR, the burden of proof is vested in controllers, who must show compelling grounds for continuing the processing.[594] Similarly, the Explanatory Report of Modernised Convention 108 clarifies that the legitimate grounds for data processing (which may override the data subjects' right to object) will have to be demonstrated on a case-by-case basis.[595]

Example: In *Manni*,[596] the CJEU held that because of the legitimate purpose of the disclosure of personal data in the company registry, in particular the need to protect the interests of third parties and ensure legal certainty, in principle, Mr Manni did not have a right to obtain the erasure of his personal data from the company registry. However, it acknowledged the existence of a right to object to the processing, by stating that "it cannot be excluded [...] that there may be specific situations in which the overriding and legitimate reasons relating to the specific case of the person concerned justify exceptionally that access to personal data entered in the register is limited, upon the expiry of a sufficiently long period [...] to third parties who can demonstrate a specific interest in their consultation".

The CJEU considered it to be the responsibility of the national courts to assess each case, taking into account all the individual's relevant circumstances and whether there existed legitimate and overriding reasons which could exceptionally justify third parties' restricted access to personal data contained

592 Modernised Convention 108, Art. 9 (1) (d); Profiling Recommendation, Art. 5 (3).

593 CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 May 2014 para. 81.

594 Also see Modernised Convention 108, Art.98 (1) (d) stating that the data subject can object to the processing of his or her data "unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms".

595 Explanatory Report of Modernised Convention 108, para. 78.

596 CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 9 March 2017, paras. 47 and 60.

in company registries. However, it clarified that in the case of Mr Manni, the mere fact that disclosure of his personal data in the register allegedly affected his clientele, cannot be considered as constituting such a legitimate and overriding reason. Potential clients of Mr Manni have a legitimate interest in having access to the information about the bankruptcy of his old company.

The effect of a successful objection is that the controller may no longer process the data in question. Processing operations performed on the data subject's data prior to the objection, however, remain legitimate.

The right to object to processing of data for direct marketing purposes

Article 21 (2) of the GDPR provides for a specific right to object to the use of personal data for the purposes of direct marketing, bringing further clarification to Article 13 of the e-Privacy Directive. Such a right is also laid down in the Modernised Convention 108, as well as in the CoE Direct Marketing Recommendation.[597] The Explanatory Report of Modernised Convention 108 clarifies that objections to data processing for direct marketing purposes should lead to unconditional erasure or removal of the personal data in question.[598]

The data subject has the right to object to the use of his or her personal data for direct marketing purposes at any time and free of charge. Data subjects must be informed of this right in a clear manner, separate from any other information.

The right to object by automated means

Where personal information is used and processed for information society services, the data subject may exercise his or her right to object to the processing of his or her personal data by automated means.

Information society services are defined as any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.[599]

597 Council of Europe, Committee of Ministers (1985), Recommendation Rec(85)20 to member states on the protection of personal data used for the purposes of direct marketing, 25 October 1985, Art. 4 (1).

598 Explanatory Report of Modernised Convention 108, para. 79.

599 Directive 98/34/EC as amended by Directive 98/48/EC laying down a procedure for the provision of information in the field of technical standards and regulations, Art. 1 (2).

Data controllers offering information society services must have in place appropriate technical arrangements and procedures to ensure that the right to object by automated means can be exercised effectively.[600] For example, this may involve blocking cookies on web pages or turning off the tracking of internet browsing.

The right to object for scientific or historical research purposes or statistical purposes

Under EU law, scientific research should be interpreted in a broad manner, including, for example, technological development and demonstration, fundamental research, applied research and privately funded research.[601] Historical research also include research for genealogical purposes, bearing in mind that the regulation should not apply to deceased persons.[602] Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results.[603] Again, the particular situation of a data subject is the legal basis regarding the right to object to personal data processing for research purposes.[604] The only exception is the necessity of the processing for the performance of a task carried out for reasons of public interest. However, the right to erasure shall not apply when processing is necessary (with or without reasons of public interest) for scientific or historical research purposes or statistical purposes.[605]

The GDPR balances the requirements of scientific, statistical or historical research and the rights of data subjects with specific safeguards and derogations in Article 89. Thus, Union or Member State law may provide derogations of the right to object insofar as such right is likely to render impossible or seriously impair the achievement of the research purposes, and if such derogations are necessary for the fulfilment of those purposes.

Under **CoE law**, Article 9 (2) of Modernised Convention 108 establishes that restrictions on the data subjects' rights, including the right to object, may be provided for by law regarding data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes when there is no

600 General Data Protection Regulation, Art. 21 (5).

601 *Ibid.*, Recital 159.

602 *Ibid.*, Recital 160.

603 *Ibid.,* Recital 162.

604 *Ibid.,* Art. 21 (6).

605 *Ibid.*, Art. 17 (3) (d).

recognisable risk of infringement of the rights and fundamental freedoms of data subjects.

However, the Explanatory Report (paragraph 41) also recognises that data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent that the intended purpose allows, and object in case they perceived the processing to excessively encroach on their rights and freedoms without a legitimate ground.

In other words, such processing would therefore be considered a priori compatible provided that other safeguards exist and that the operations, in principle, exclude any use of the information obtained for decisions or measures concerning a particular individual.

6.1.7. Automated individual decision-making, including profiling

Automated decisions are decisions taken using personal data processed solely by automatic means without any human intervention. **Under EU law**, data subjects must not be subject to automated decisions which produce legal effects or have similarly significant effects. If such decisions are likely to have a significant impact on the lives of individuals as they relate, for example, to creditworthiness, e-recruitment, performance at work, or the analysis of conduct or reliability, then special protection is necessary to avoid negative consequences. Automated decision-making includes profiling, which consists of any form of automatic evaluation of "personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements".[606]

Example: To quickly assess the creditworthiness of a future customer, credit reference agencies (CRAs) gather certain data, such as how the customer has maintained his or her credit and service/utility accounts, the details of customer's previous addresses as well as information from public sources, such as electoral roll, public records (including court judgments), or bankruptcy and insolvency data. These personal data are subsequently fed

606 *Ibid*., Recital 71, Art. 4 (4) and Art. 22.

into a scoring algorithm, which calculates an overall value representing the creditworthiness of the potential customer.

According to the Article 29 Working Party, the right not to be subject to decisions based solely on automated processing that may result in legal effects for the data subject or that significantly affect him or her equates to a general prohibition and does not require the data subject to proactively seek an objection to such a decision.[607]

Nevertheless, according to the GDPR, automated decision-making with legal effects or that significantly affect individuals may be acceptable if it is necessary for entering a contract or the performance of a contract between the data controller and data subject, or if the data subject gave explicit consent. Also, automated decision-making is acceptable if it is authorised by law and if the data subject's rights, freedoms and legitimate interests are appropriately safeguarded.[608]

The GDPR also provides that among the controller's obligations regarding the information to be provided where personal data are collected, data subjects must be told about the existence of automated decision-making, including profiling.[609] The right to access the personal data processed by the controller remains unaffected.[610] The information should not only indicate the fact that profiling will occur, it should also contain meaningful information about the logic involved in the profiling and the envisaged consequences for individuals of the processing.[611] For instance, a health insurance company using automated decision-making on applications should provide data subjects with general information on how the algorithm works, and which factors the algorithm uses to calculate their insurance premiums. Similarly, when exercising their 'right of access', data subjects can request information from the controller on the existence of automated decision-making and meaningful information about the logic involved.[612]

The information provided to data subjects is intended to provide transparency and enable data subjects to provide informed consent, if that is the case, or to obtain human intervention. The data controller is required to implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests. This

607 Article 29 Working Party, *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 3 October 2017, p. 15.

608 General Data Protection Regulation, Art. 22 (2).

609 *Ibid.*, Art. 12.

610 *Ibid.*, Art. 15.

611 *Ibid.*, Art. 13 (2) (f).

612 *Ibid.*, Art. 15 (1) (h).

includes at least the right to obtain human intervention on the part of the controller and the possibility for the data subject to express a point of view and to contest a decision based on the automated processing of their personal data.[613]

The Article 29 Working Party has provided further guidance on the use of automated decision-making under the GDPR.[614]

Under CoE law, individuals have a right not to be subject to a decision which will significantly affect them and which is based solely on automated processing without having their views taken into consideration.[615] The requirement to consider the data subject's views when decisions are based solely on automated processing means that they have a right to challenge such decisions, and should be able to contest any inaccuracy in the personal data the controller uses, and challenge whether any profile applied to them is relevant.[616] However, an individual cannot exercise this right if the automated decision is authorised by a law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests. In addition, data subjects have the right to obtain, upon request, knowledge of the reasoning underlying the data processing carried out.[617] The Explanatory Report of Modernised Convention 108 gives the example of credit scoring. Individuals should be entitled to know not only the positive or negative scoring decision itself but also the *logic* underpinning the processing of their personal data, which resulted in such a decision. "Having an understanding of these elements contributes to the effective exercise of other essential safeguards such as the right to object and the right to complain to a competent authority".[618]

The Profiling Recommendation, albeit not legally binding, specifies the conditions for the collection and processing of personal data in the context of profiling.[619] It includes provisions on the need to ensure that the processing in the context of profiling should be fair, lawful, proportionate and for specified and legitimate

613 *Ibid*., Art. 22 (3).

614 Article 29 Working Party (2017), *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,* WP 251, 3 October 2017.

615 Modernised Convention 108, Art. 9 (1) (a).

616 Explanatory Report of Modernised Convention 108, para. 75.

617 Modernised Convention 108, Art. 9 (1) (c).

618 Explanatory Report of Modernised Convention 108, para. 77.

619 Council of Europe, Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, Art. 5 (5).

purposes. It also includes provisions on the information controllers should provide to data subjects. The data quality principle – which requires controllers to take measures to correct data inaccuracy factors, to limit the risks or errors that profiling may entail, and to periodically evaluate the quality of the data and algorithms used – also features in the recommendation.

6.2. Remedies, liability, penalties and compensation

Key points

- According to Modernised Convention 108, the national law of the Contracting Parties must set out appropriate remedies and sanctions against infringements of the right to data protection.
- In the EU, the GDPR provides for remedies for data subjects in cases of violation of their rights, as well as for sanctions against controllers and processors who do not comply with the provisions of the regulation. It also provides for the right to compensation and liability.
    - Data subjects have the right to lodge a complaint to a supervisory authority for alleged infringements of the regulation, as well as the right to an effective judicial remedy and to receive compensation.
    - In the exercise of their right to an effective remedy, individuals may be represented by non-profit organisations active in the field of data protection.
    - The controller or processor is liable for any material and non-material damage as a result of the infringement.
    - The supervisory authorities have the power to impose administrative fines for infringements of the regulation up to € 20,000,000 or in the case of an undertaking, 4 % of the total worldwide annual turnover – whichever is higher.
- Data subjects may bring violations of data protection law, as a last resort and under certain conditions, before the ECtHR.
- Any natural or legal person has the right to bring an action for annulment of decisions of the European Data Protection Board before the CJEU under the conditions provided for in the Treaties.

Adopting legal instruments is not sufficient to ensure the protection of personal data within Europe. To make European data protection rules effective, it is necessary to

establish mechanisms that enable individuals to counter violations of their rights and to seek compensation for any damage suffered. It is also important that supervisory authorities have the power to impose sanctions that are effective, dissuasive and proportionate to the infringement in question.

Rights under data protection law can be exercised by the person whose rights are at stake; this will be someone who is the data subject. However, other persons – who fulfil the necessary requirements under national law – may also represent data subjects in exercising their rights. Under a number of national legislations, children and persons with intellectual disabilities must be represented by their guardians.[620] Under EU data protection law, an association – whose lawful aim is to promote data protection rights – may represent data subjects before a supervisory authority or a court.[621]

6.2.1. Right to lodge a complaint with a supervisory authority

Under both **CoE** and **EU law**, individuals have the right to lodge requests and complaints to the competent supervisory authority if they consider that the processing of their personal data is not being carried out in accordance with the law.

Modernised Convention 108 recognises the right of data subjects to benefit from the assistance of a supervisory authority in exercising their rights under the convention, irrespective of their nationality or residence.[622] A request for assistance may only be rejected in exceptional circumstances, and data subjects should not cover the costs and fees related to the assistance.[623]

Similar provisions can be found in the EU legal system. The GDPR requires supervisory authorities to adopt measures to facilitate the submission of complaints, such as the creation of an electronic complaint submission form.[624] The data subject can lodge the complaint with the supervisory authority in the Member State of his or her

620 FRA (2015), Handbook on European law relating to the rights of the child, Luxembourg, Publications Office; FRA (2013), Legal capacity of persons with intellectual disabilities and persons with mental health problems, Luxembourg, Publications Office.

621 General Data Protection Regulation, Art. 80.

622 Modernised Convention 108, Art. 18.

623 *Ibid*., Art. 16–17.

624 General Data Protection Regulation, Art. 57 (2).

habitual residence, place of work, or place of the alleged infringement.[625] Complaints must be investigated, and the supervisory authority must inform the person concerned of the outcome of the proceedings dealing with the claim.[626]

Potential infringements by EU institutions or bodies can be brought to the attention of the European Data Protection Supervisor.[627] In the absence of a response from the EDPS within six months, the complaint shall be deemed to have been rejected. Appeals against the EDPS' decisions can be brought before the CJEU within the framework of Regulation (EC) No. 45/2001 conferring an obligation to comply with data protection rules to EU institutions and bodies.

There must be the possibility to appeal to the courts against decisions by a national supervisory authority. This applies to the data subject as well as to controllers and processors that have been a party to proceedings before a supervisory authority.

Example: In September 2017, the Spanish Data Protection Authority fined Facebook for violating several data protection regulations. The supervisory authority condemned the social network for collecting, storing and processing personal data, including special categories of personal data, for advertising purposes and without obtaining data subject's consent. The decision was based on an investigation conducted on the supervisory authority's own initiative.

6.2.2. Right to an effective judicial remedy

In addition to the right to complain to the supervisory authority, individuals must have the right to an effective judicial remedy and to bring their case before a court. The right to a legal remedy is well-enshrined in the European legal tradition, and is recognised as a fundamental right, both under Article 47 of the EU Charter of Fundamental Rights and Article 13 of the ECHR.[628]

625 *Ibid.*, Art. 77 (1).

626 *Ibid.*, Art. 77 (2).

627 Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, OJ 2001 L 8.

628 See for example ECtHR, *Karabeyoğlu v. Turkey*, No. 30083/10, 7 June 2016; ECtHR, *Mustafa Sezgin Tanrıkulu v. Turkey*, No. 27473/06, 18 July 2017.

Under EU law, the importance of providing data subjects with effective legal remedies in case there is a violation of their rights is clear from both the provisions of the GDPR – which establishes a right to an effective judicial remedy against supervisory authorities, controllers and processors – and from CJEU case law.

> Example: In *Schrems*,[629] the CJEU declared the Safe Harbour Adequacy Decision invalid. That decision had allowed international data transfers from the EU to organisations in the US that self-certified under the Safe Harbour scheme. The CJEU considered the Safe Harbour scheme to have several shortcomings, which compromised EU citizens' fundamental rights to the protection of privacy, the protection of personal data and the right to an effective legal remedy.
>
> Concerning the violation of the rights to privacy and data protection, the CJEU highlighted that US legislation permitted certain public authorities to access the personal data transferred from the Member States to the US and process it in a way that was incompatible with its original transfer purposes and beyond what was strictly necessary and proportionate to the protection of national security. On the right to an effective remedy, it noted that the data subjects had no administrative or judicial means of redress to enable the data relating to them to be accessed and rectified or erased, as the case may be. The CJEU concluded that legislation not providing for any possibility of pursuing legal remedies to access, rectify or erase their personal data "does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter". It highlighted that the existence of a judicial remedy guaranteeing compliance with legal rules is inherent in the rule of law.

Individuals, controllers or processors seeking to challenge a supervisory authority's legally binding decision may bring proceedings before a court.[630] The term 'decision' should be interpreted broadly, covering supervisory authorities' exercise of investigative, sanctioning and authorisation powers, as well as decisions to dismiss or reject a complaint. However, non-legally binding measures, such as opinions or advice given by the supervisory authority cannot form the subject matter of an

629 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 6 October 2015.

630 General Data Protection Regulation, Art. 78.

action before a court.[631] The court action must be brought before the courts of the Member State where the relevant supervisory authority is established.[632]

In cases where a controller or processor infringe a data subject's rights, data subjects are entitled to bring a complaint before a court.[633] For proceedings initiated against a controller or processor, it is particularly important that individuals are given the option to choose where to bring the action. They may choose to do so either in the Member State in which the controller or processor has an establishment, or in the Member State in which the data subjects concerned have their habitual residence.[634] The second possibility greatly facilitates individuals in exercising their rights, as it enables them to bring actions in the state where they reside and within a familiar jurisdiction. Restricting the venue for proceedings against controllers and processors to the Member State in which the latter have an establishment could discourage data subjects residing in other Member States from bringing a court action, as it would entail travelling and additional costs, and the proceedings could be in a foreign language and jurisdiction. The only exception concerns cases where the controller or processor are public authorities and processing is undertaken in the exercise of their public powers. In this case, only the courts of the state of the relevant public authority are competent for a claim.[635]

While, in most instances, cases concerning data protection rules will be decided in the courts of the Member States, some cases may be brought before the CJEU. The first possibility is where a data subject, a controller, processor or supervisory authority seeks an action for annulment of an EDPB decision. The action, however, is subject to the conditions of Article 263 of the TFEU, which means that in order to be admissible, these individuals and entities need to demonstrate that the Board decision is of direct and individual concern to them.

The second scenario concerns cases of EU institutions or bodies unlawfully processing personal data. In cases where EU institutions infringe data protection law, data subjects can bring a claim directly in front of the General Court of the EU (the General Court is part of the CJEU). The General Court is, in the first instance, responsible for

631 *Ibid.*, Recital 143.

632 *Ibid.*, Art. 78 (223).

633 *Ibid.*, Art. 79.

634 *Ibid.*, Art. 79 (2).

635 *Ibid.*

complaints of infringements of EU law by EU institutions. Thus, complaints against the EDPS – as an EU institution – can be brought before the General Court as well.[636]

Example: In *Bavarian Lager*,[637] the company asked the European Commission to provide access to the full minutes of a meeting the Commission held which allegedly related to legal questions relevant to the company. The Commission rejected the company's request for access on grounds of overriding data protection interests.[638] Bavarian Lager, under Article 32 of the EU Institutions Data Protection Regulation, brought a complaint before the Court of First Instance (the forerunner of the General Court) regarding that decision. In its decision (case T194/04, *The Bavarian Lager Co. Ltd v. Commission of the European Communities*), the Court of First Instance annulled the decision of the Commission to reject the access request. The European Commission appealed this decision to the CJEU.

The CJEU gave judgment (in the Grand Chamber) setting aside the judgment of the Court of First Instance and confirming the European Commission's rejection of the request for access to the full minutes of the meeting, in order to protect the personal data of the persons at the meeting. The CJEU considered the Commission correct in refusing to disclose that information, given that the participants had not given their consent to the disclosure of their personal data. In addition, Bavarian Lager had not demonstrated the necessity of accessing that information.

Finally, data subjects, supervisory authorities, controllers or processors may, in the course of domestic proceedings, ask the national court to request clarification from the CJEU on the interpretation and validity of acts of EU institutions, bodies, offices or agencies. Such clarifications are known as preliminary rulings. This is not a direct remedy for the complainant, but it enables national courts to ensure that they apply the correct interpretation of EU law. It is through this mechanism of preliminary rulings that seminal cases – such as *Digital Rights Ireland and Kärntner Landesregierung*

636 Regulation (EC) No. 45/2001, Art. 32 (3).

637 CJEU, C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd* [GC], 2010.

638 For an analysis of the argument, see EDPS (2011), *Public access to documents containing personal data after the Bavarian Lager ruling*, Brussels, EDPS.

and Others[639] and *Schrems*[640] – which greatly affected the development of EU data protection law, reached the CJEU.

Example: *Digital Rights Ireland* and *Kärntner Landesregierung and Others*[641] was a joined case submitted by the Irish High Court and the Austrian Constitutional Court concerning the conformity of Directive 2006/24/EC (Data Retention Directive) with EU data protection law. The Austrian Constitutional Court submitted questions to the CJEU concerning the validity of Articles 3 to 9 of Directive 2006/24/EC in light of Articles 7, 9 and 11 of the EU Charter of Fundamental Rights. These included whether or not certain provisions of the Austrian Federal Law on Telecommunications transposing the Data Retention Directive were incompatible with aspects of the former Data Protection Directive and the EU Institutions Data Protection Regulation.

In the case of *Kärntner Landesregierung and Others,* Mr Seitlinger – one of the applicants in the Constitutional Court proceeding – held that he used the telephone, the internet and email both for work purposes and in his private life. Consequently, the information he sent and received passed through public telecommunication networks. Under the Austrian Telecommunications Act of 2003, his telecommunications provider was legally required to collect and store data about his use of the network. Mr Seitlinger believed this collection and storage of his personal data to be unnecessary for the technical purposes of sending and receiving information via the network. Nor, indeed, was the collection and storage of these data necessary for billing purposes. Mr Seitlinger stated that he had not consented to this use of his personal data, which were solely collected and stored on account of the Austrian Telecommunications Act of 2003.

Mr Seitlinger therefore brought an action before the Austrian Constitutional Court, in which he alleged that the statutory obligations on his telecommunications' provider breached his fundamental rights under Article 8 of the EU Charter of Fundamental Rights. Given that the Austrian legislation implemented EU law (the then Data Retention Directive), the

639 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [GC], 8 April 2014.

640 CJEU, C-362/14, *Maximilian Schrems v. Data Protection Commissioner* [GC], 6 October 2015.

641 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [GC], 8 April 2014.

Austrian Constitutional Court referred the matter to the CJEU to decide the compatibility of the directive with the rights to privacy and data protection enshrined in the EU Charter of Fundamental Rights.

The CJEU Grand Chamber decided the case, which resulted in the annulment of the EU Data Retention Directive. The CJEU found that the directive entailed a particularly serious interference with the fundamental rights to privacy and data protection, without that interference being limited to what is strictly necessary. The directive pursued a legitimate aim, as it allowed national authorities to have additional opportunities to investigate and prosecute serious crimes and was thus a valuable tool for criminal investigations. However, the CJEU noted that limitations to fundamental rights should apply only if strictly necessary and should be accompanied with clear and precise rules regarding their scope, together with safeguards for individuals.

According to the CJEU, the directive failed to meet this necessity test. Firstly, it did not establish clear and precise rules limiting the extent of the interference. Instead of requiring a relationship between the retained data and serious crime, the directive applied to all metadata of all users of all electronic communication means. It thus constituted an interference with the rights to privacy and data protection of practically the entire EU population, which could be considered disproportionate. It did not contain conditions to limit the persons authorised to access the personal data, nor was such access subject to procedural conditions such as the requirement to have the approval of an administrative authority or court prior to access. Finally, the directive did not set out clear safeguards for the protection of retained data. It therefore failed to ensure effective protection of the data against the risk of abuse and against any unlawful access and use of the data.[642]

In principle, the CJEU must answer referred questions and it cannot refuse to give its preliminary ruling on the grounds that this response would be neither relevant nor timely in respect of the original case. It can, however, refuse if the question does not fall within its sphere of competence.[643] The CJEU gives a decision only on

642 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [GC], 8 April 2014, para. 69.

643 CJEU, C-244/80, *Pasquale Foglia v. Mariella Novello (No. 2)*, 16 December 1981; CJEU, C-467/04, *Criminal Proceedings against Gasparini and Others*, 28 September 2006.

the constituent elements of the request referred for a preliminary ruling, while the national court retains its competence to decide the original case.[644]

Under CoE law, Contracting Parties must establish appropriate judicial and non-judicial remedies for violations of the provisions of Modernised Convention 108.[645] Allegations data protection rights violations contravening Article 8 of the ECHR against a Contracting Party to the ECHR, may, additionally, be brought before the ECtHR when all available domestic remedies have been exhausted. A plea of violation of Article 8 of the ECHR before the ECtHR must also meet other admissibility criteria (Articles 34–35 of the ECHR).[646]

Although applications to the ECtHR can be directed only against Contracting Parties, they can also indirectly deal with actions or omissions of private parties, insofar as a Contracting Party has not fulfilled its positive obligations under the ECHR and has not provided sufficient protection against infringements of data protection rights in its national law.

Example: In *K.U. v. Finland*,[647] the applicant – a minor – complained that an advertisement of a sexual nature had been posted about him on an internet dating site. The service provider did not reveal the identity of the person who had posted the information because of confidentiality obligations under Finnish law. The applicant claimed that Finnish law did not provide sufficient protection against such actions of a private person placing incriminating data about the applicant on the internet. The ECtHR held that states were not only compelled to abstain from arbitrary interference with individuals' private lives, but may also be subject to positive obligations which involve "the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves". In the applicant's case, his practical and effective protection required that effective steps be taken to identify and prosecute the perpetrator. However, the state had not afforded such protection, and the Court concluded that there had been a violation of Article 8 of the ECHR.

644 CJEU, C-438/05, *International Transport Workers' Federation, Finnish Seamen's Union v. Viking Line ABP, OÜ Viking Line Eesti* [GC], 11 December 2007, para. 85.

645 Modernised Convention 108, Art. 12.

646 ECHR, Art. 34–37.

647 ECtHR, *K.U. v. Finland*, No. 2872/02, 2 December 2008.

Example: In *Köpke v. Germany*,[648] the applicant had been suspected of theft at her workplace and subjected to covert video surveillance. The ECtHR concluded that there was "nothing to indicate that the domestic authorities failed to strike a fair balance, within their margin of appreciation, between the applicant's right to respect for her private life under Article 8 and both her employer's interest in the protection of its property rights and the public interest in the proper administration of justice". The application was therefore declared inadmissible.

If the ECtHR finds that a Contracting Party has violated any of the rights protected by the ECHR, that Contracting Party is obliged to execute the ECtHR's judgment (Article 46 of the ECHR). Execution measures must first put an end to the violation and remedy, as far as possible, its negative consequences for the applicant. Execution of judgments may also require general measures to prevent violations similar to those found by the Court, whether through changes in legislation, case law or other measures.

Where the ECtHR finds a violation of the ECHR, Article 41 of the ECHR provides that it may award "just satisfaction" to the applicant at the expense of the Contracting Party.

Right to mandate a not-for-profit body, organisation or association

The GDPR enables individuals lodging a complaint to a supervisory authority or bringing legal action before a court to mandate a non-profit body, organisation or association to represent them.[649] These non-profit entities must have statutory objectives within the sphere of public interest and be active in the field of data protection. They may lodge the complaint or exercise the right to judicial remedy on behalf of the data subject(s). The regulation gives Member States the option to decide – in accordance with national law – whether a body can lodge complaints on behalf of data subjects, without being mandated by those data subjects.

This representation right enables individuals to benefit from the expertise and organisational and financial capacity of such non-profit entities, thereby greatly facilitating individuals in exercising their rights. The GDPR allows these entities to bring collective claims on behalf of multiple data subjects. This also benefits the functioning and efficiency of the judicial system, as similar claims are grouped and examined together.

648 ECtHR, *Köpke v. Germany* (dec.), No. 420/07, 5 October 2010.

649 General Data Protection Regulation, Art. 80.

6.2.3. Liability and the right to compensation

The right to an effective remedy must empower individuals to claim compensation for any damage suffered as a result of processing their personal data in a manner that infringes the applicable legislation. The liability of controllers and processors for unlawful processing is recognised explicitly in the GDPR.[650] The regulation gives individuals the right to receive compensation from the controller or processor for both material and non-material damages, while its recitals stipulate that "the concept of damage should be broadly interpreted in the light of the case law of the Court of Justice in a manner which fully reflects the objectives of this Regulation".[651] Controllers are liable and could be subject to compensation claims if they do not meet their obligations under the regulation. Personal data processors are liable for the damage caused by processing only where it has not complied with the regulation's obligations specifically addressed to processors, or where it has acted outside, or contrary to, the lawful instructions of the controller. If a controller or processor has paid full compensation, the GDPR provides that the controller or processor can claim back – from the other controllers or processors involved in the same processing – that part of the compensation corresponding to the degree of responsibility for the damage.[652] At the same time, exceptions from liability are very strict and subject to proof that the controller or processor is not in any way responsible for the event that gave rise to the damage.

Compensation must be 'full and effective' in relation to the damage suffered. Where damage is caused by the processing of several controllers and processors, each controller or processor must be held liable for the entire damage. This rule seeks to ensure effective compensation for data subjects and a coordinated approach to compliance by the controllers and processors involved in processing activities.

Example: Data subjects are not required to bring a case and claim compensation from all the entities responsible for the damage, as this might entail expensive and lengthy proceedings. It is sufficient to bring a case against one of the joint controllers, which may then be held liable for the full damage. In such cases, a controller or processor who pays the damage is subsequently entitled to recover the sum paid from the other entities involved in the processing and responsible for the violation, for their part of

650 *Ibid.*, Art. 82.

651 *Ibid.*, Recital 146.

652 *Ibid.*, Art. 82 (2) and (5).

the responsibility for the damage. These proceedings between the different joint controllers and processors take place after the data subject has received compensation and the data subject is not part of them.

In the CoE legal framework, Article 12 of Modernised Convention 108 requires Contracting Parties to establish appropriate remedies for violations of national law implementing the convention's requirements. The Explanatory Report of Modernised Convention 108 indicates that remedies must include the possibility to judicially challenge a decision or practice, while non-judicial remedies must also be made available.[653] The modalities and different rules related to the access of these remedies, together with the procedure to be followed, are left to the discretion of each Contracting Party. Contracting Parties and national courts should also consider financial compensation provisions for material and non-material damages caused by the processing, as well as the possibility of enabling collective actions.[654]

6.2.4. Sanctions

Under CoE law, Article 12 of Modernised Convention 108 provides that appropriate sanctions and remedies must be established by each Contracting Party for violations of domestic law provisions that give effect to the basic principles of data protection set out in Convention 108. The convention does not establish or impose a particular set of sanctions. On the contrary, it clearly indicates that each Contracting Party has the discretion to determine the nature of judicial or non-judicial sanctions, which may be criminal, administrative or civil. The Explanatory Report of Modernised Convention 108 provides that sanctions must be effective, proportionate and dissuasive.[655] Contracting Parties must respect this principle when determining the nature and severity of sanctions available in their domestic legal order.

Under EU law, Article 83 of the GDPR empowers Member States' supervisory authorities to impose administrative fines for infringements of the regulation. The level of fines, and the circumstances that national authorities take into account when deciding whether to impose a fine, as well as the total maximum ceilings of that fine, are also provided for in Article 83. The sanctioning regime is thus harmonised across the EU.

653 Explanatory Report of Modernised Convention 108, para. 100.

654 *Ibid*.

655 *Ibid*.

The GDPR follows a tiered approach to fines. The supervisory authorities have the power to impose administrative fines for infringements of the regulation of up to € 20,000,000 or, in the case of an undertaking, 4 % of its total worldwide annual turnover – whichever is higher. Infringements that can trigger this level of fine include breaches of the basic principles for processing and the conditions for consent, breaches of data subjects' rights and of the regulation's provisions governing the transfer of personal data to recipients in third countries. For other infringements, supervisory authorities may impose fines of up to € 10,000,000 or, in the case of an undertaking, two percent of its total worldwide annual turnover – whichever is higher.

When determining the type and level of fine to be imposed, supervisory authorities must take a series of factors into account.[656] For instance, they must duly consider the nature, gravity and duration of the infringement, the categories of personal data affected, and whether it had an intentional or negligent character. Where a controller or processor has taken action to mitigate the damage suffered by data subjects, this should also be taken into consideration. Similarly, the degree of cooperation with the supervisory authority following the infringement, and the manner in which the supervisory authority learned of the infringement (for example, whether it was reported by the entity responsible for the processing, or by a data subject whose rights were violated) are other important factors guiding the supervisory authorities in their decision.[657]

In addition to the ability to impose administrative fines, supervisory authorities have a wide range of other corrective powers at their disposal. The so-called 'corrective' powers of the supervisory authorities are set out in Article 58 of the GDPR. They range from the issuing of orders, warnings and reprimands to controllers and processors, to the imposition of temporary or even permanent bans on processing activities.

Regarding the sanctions against infringements of EU law by EU institutions or bodies, because of the special remit of the EU institutions Data Protection Regulation, sanctions may be envisaged in the form of disciplinary action. According to Article 49 of the regulation, "any failure to comply with the obligations pursuant to this Regulation, whether intentionally or through negligence on his or her part, shall make an official or other servant of the European Communities liable to disciplinary action [...]".

656 General Data Protection Regulation, Art. 83 (2).

657 Article 29 Working Party (2017), *Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679*, WP 253, 3 October 2017.

7

International data transfers and flows of personal data

EU	Issues covered	CoE
Personal data transfers		
General Data Protection Regulation, Article 44	Concept	Modernised Convention 108, Article 14 (1) and (2)
Free flow of personal data		
General Data Protection Regulation, Article 1 (3) and Recital 170	Between EU Member States	
	Between Contracting Parties to Convention 108	Modernised Convention 108, Article 14 (1)
Personal data transfers to third countries or international organisations		
General Data Protection Regulation, Article 45 C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 2015	Adequacy decision/third countries or international organisations with appropriate levels of protection	Modernised Convention 108, Article 14 (2)
General Data Protection Regulation, Article 46 (1) and 46 (2)	Appropriate safeguards, including enforceable rights and legal remedies for data subjects, provided through standard contractual clauses, binding corporate rules, codes of conduct and certification mechanisms	Modernised Convention 108, Article 14 (2), (3), (5) and (6)

EU	Issues covered	CoE
General Data Protection Regulation, Article 46 (3)	Subject to the authorisation from the competent supervisory authority: contractual clauses and provisions included in administrative arrangements between public authorities	
General Data Protection Regulation, Article 46 (5)	Existing authorisations on the basis of Directive 95/46	
General Data Protection Regulation, Article 47	Binding corporate rules	
General Data Protection Regulation, Article 49	Derogations for specific situations	Modernised Convention 108, Article 14 (4)
Examples: EU–US PNR Agreement EU–US SWIFT Agreement	International agreements	Modernised Convention 108, Article 14 (3) (a)

Under EU law, the General Data Protection Regulation provides for the free flow of data within the European Union. However, it contains specific requirements relating to the personal data transfers to third countries outside the EU and to international organisations. The regulation recognises the importance of such transfers, especially in view of international trade and cooperation, but also recognises the increased risk to personal data. The regulation therefore aims to offer the same level of protection to personal data being transferred to third countries as they enjoy within the EU.[658] CoE law also recognises the importance of implementing rules for transborder data flows, based on a free flow between parties and specific requirements for transfers to non-parties.

7.1. Nature of personal data transfers

Key points

- EU and CoE laws have rules on personal data transfers to recipients in third countries or to international organisations.
- Ensuring the data subject's rights are safeguarded when data are transferred outside the EU allows the protection afforded by EU law to follow the personal data originating in the EU.

658 General Data Protection Regulation, Recitals 101 and 116.

Under **CoE law**, transborder data flows are described as personal data transfers to recipients who are subject to a foreign jurisdiction.[659] Transborder data flows to a recipient who is not subject to the jurisdiction of a Contracting Party are only allowed if there is an appropriate level of protection.[660]

EU law regulates transfers "of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation [...]".[661] Such data flows are only allowed if they comply with the rules set out in Chapter V of the GDPR.

Cross-border flows of personal data are allowed to a recipient who is subject to the jurisdiction of a Contracting Party or Member State under CoE law or EU law, respectively. Both legal systems also allow data to be transferred to a country that is not a Contracting Party or a Member State, provided that certain conditions are fulfilled.

7.2. Free movement/flow of personal data between Member States or Contracting Parties

Key points

- The flow of personal data throughout the EU, as well as personal data transfers among Contracting Parties to Modernised Convention 108, must be free from restrictions. However, as not all Contracting Parties to Modernised Convention 108 are Member States of the EU, transfers from an EU Member State to a third country that is, nevertheless, a Contracting Party to Convention 108, are not possible unless they meet the conditions set out in the GDPR.

Under CoE law, there must be a free flow of personal data between Contracting Parties to Modernised Convention 108. However, the transfer may be prohibited if there is a "real and serious risk that the transfer to another Party would lead to circumventing the provisions of the Convention" or if a Party is bound to do so by

659 Explanatory Report of Modernised Convention 108, para. 102.

660 Modernised Convention 108, Art. 14 (2).

661 General Data Protection Regulation, Art. 44.

"harmonised rules of protection shared by States belonging to a regional international organisation".[662]

Under EU law, restrictions or prohibitions on the free movement of personal data between EU Member States for reasons connected with the protection of natural persons regarding personal data processing are forbidden.[663] **The area of free data flow has been extended by the** Agreement on the European Economic Area (EEA),[664] which brings Iceland, Liechtenstein and Norway into the internal market.

Example: If an affiliate of an international group of companies, being established in several Member States, amongst them Slovenia and France, sends personal data from Slovenia to France, such a data flow must not be restricted or prohibited by Slovenian national law for reasons connected with personal data protection.

If, however, the same Slovenian affiliate wants to transfer the same personal data to the parent company in Malaysia, then the Slovenian data exporter must take into account the rules in Chapter V of the GDPR. These provisions are intended to safeguard the personal data of data subjects who are subject to EU jurisdiction.

Under EU law, flows of personal data to Member States of the EEA for purposes related to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties are subject to Directive 2016/680.[665] This also ensures that the exchange of personal data by competent authorities within the Union is not restricted or prohibited for data protection reasons. Under CoE law, processing of all personal data (including their cross-border flow with other parties to Convention 108), with no exceptions based on purposes or fields of action, are

662 Modernised Convention 108, Art. 14 (1).

663 General Data Protection Regulation, Art. 1 (3).

664 Decision of the Council and the Commission of 13 December 1993 on the conclusion of the Agreement on the European Economic Area between the European Communities, their Member States and the Republic of Austria, the Republic of Finland, the Republic of Iceland, the Principality of Liechtenstein, the Kingdom of Norway, the Kingdom of Sweden and the Swiss Confederation, OJ 1994 L 1.

665 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L119.

included within the scope of Convention 108, although exemptions may be made by the Contracting Parties. All members of the EEA are also parties to Convention 108.

7.3. Personal data transfers to third countries/non-parties or to international organisations

Key points

- Both the **CoE** and the **EU** allow for personal data transfers to third countries or international organisations, provided that certain conditions are met for the protection of personal data.
  - **Under CoE law**, an appropriate level of protection can be achieved by the law of the State or international organisation or by having appropriate standards in place.
  - **Under EU law**, transfers may take place if the third country ensures an adequate level of protection or if the data controller or processor provides appropriate safeguards, including enforceable data subject rights and legal remedies, through means such as standard data protection clauses or binding corporate rules.
- **Both CoE law and EU law** provide for derogation clauses allowing for the transfer of personal data in specific circumstances even where neither an adequate level of protection nor appropriate safeguards are in place.

While both CoE law and EU law allow for data flows to third countries or to international organisations, they lay down different conditions. Each set of conditions takes account of the respective organisation's different structure and purposes.

Under **EU law**, there are, in principle, two ways of allowing the transfer of personal data to third countries or to international organisations. Transfers of personal data may take place on the basis of: an adequacy decision by the European Commission;[666] or, in the absence of such an adequacy decision, where the controller or processor provides appropriate safeguards, including enforceable rights and legal remedies for the data subject.[667] In the absence of either an adequacy decision or appropriate safeguards, a number of derogations are available.

666 General Data Protection Regulation, Art. 45.

667 *Ibid.*, Art. 46.

Under **CoE** law, however, free data transfers to non-parties to the convention are only allowed on the basis of:

- the law of that state or international organisation, including the applicable international treaties or agreements guaranteeing appropriate safeguards;
- ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing.[668]

Similarly to EU law, in the absence of an appropriate level of data protection, a number of derogations are available.

7.3.1. Transfers on the basis of an adequacy decision

Under EU law, the free flow of personal data to third countries with an adequate level of data protection is provided for in Article 45 of the GDPR. The CJEU has clarified that the term "adequate level of protection" requires the third country to ensure a level of protection of fundamental rights and freedoms that is "essentially equivalent"[669] to the guarantees ensured by law in the EU. At the same time, the means to which a third country has recourse for the purposes of ensuring such a level of protection may differ from those employed within the EU, the adequacy standard does not require a point-to-point replication of EU rules.[670]

The European Commission assesses the level of data protection in foreign countries by looking at their national law and applicable international obligations. A country's participation in multilateral or regional systems, in particular regarding the protection of personal data, is to be taken into account as well. If the European Commission finds that the third country or international organisation ensures an adequate level of protection, it can issue an adequacy decision which has binding effect.[671] Nevertheless, the CJEU has stated that national supervisory authorities still have the competence to examine the claim of a person concerning the protection of their

668 Modernised Convention 108, Art. 14 (3) (a) and (b).

669 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 6 October 2015, para. 96.

670 *Ibid.*, para. 74. See also, European Commission (2017), Communication from the Commission to the European Parliament and the Council "Exchanging and Protection Personal Data in a Globalised World", COM(2017)7 final of 10 January 2017, p. 6.

671 For a continually updated list of countries that have received a finding of adequacy, see the homepage of the European Commission, Directorate-General for Justice.

personal data which has been transferred to a third country that has been deemed by the Commission as ensuring an adequate level of protection, where that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.[672]

The European Commission can also assess the adequacy of a territory within a third country, or confine itself to specific sectors, as was the case for Canada's private commercial legislation, for example.[673] There are also adequacy findings for transfers based on agreements between the EU and third countries. These decisions refer exclusively to a single type of data transfer, such as an airline's transmission of passenger name records (PNR) to foreign border control authorities when the airline flies from the EU to certain overseas destinations (see Section 7.3.4).

Adequacy decisions are subject to monitoring on an ongoing basis. The European Commission regularly reviews such decisions to track developments that could affect their status. Thus, if the European Commission finds that the third country or international organisation no longer meet the conditions justifying the adequacy decision, it can amend, suspend or repeal the decision. The Commission may also enter into negotiations with the third country or international organisation concerned to remedy the issue behind its decision.

Adequacy decisions adopted by the European Commission on the basis of Directive 95/46/EC remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with the rules in Article 45 of the GDPR.

To date, the European Commission has recognised Andorra, Argentina, Canada (commercial organisations falling under the scope of the Personal Information and Electronic Documents Act – PIPEDA), Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay as providing adequate protection. With respect to transfers to the US, the European Commission adopted an adequacy decision in 2000 allowing transfers to companies that self-certified their protection of personal data transferred from the EU and compliance with the so-called 'Safe

672 CJEU, C-362/14, *Maximilian Schrems v. Data Protection Commissioner* [GC], 6 October 2015, paras. 63 and 65–66.

673 European Commission (2002), Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, OJ 2002 L 2.

Harbour principles'.[674] The CJEU invalidated this decision in 2015 and a new adequacy decision was adopted in July 2016, allowing companies to join as of 1 August 2016.

Example: In *Schrems,*[675] Maximilian Schrems, an Austrian citizen, had been a Facebook user for several years. Some or all of the data provided by Mr Schrems to Facebook were transferred from Facebook's Irish subsidiary to servers located in the US, where they were processed. Mr Schrems lodged a complaint with the Irish data protection authority, taking the view that, in light of the revelations that US whistleblower Edward Snowden made concerning the US intelligence services' surveillance activities, US law and practice does not offer sufficient protection of the data transferred to that country. The Irish authority rejected the complaint, on the ground that, in its decision of 26 July 2000, the Commission considered that, under the 'Safe Harbour' scheme, the US ensures an adequate level of protection of the personal data transferred. The case was brought before the Irish High Court, which referred it to the CJEU for a preliminary ruling.

The CJEU ruled that the Commission's decision on the adequacy of the Safe Harbour framework was invalid. The CJEU first noted that the decision allowed the applicability of the Safe Harbour data protection principles to be limited on the basis of national security, public interest or law enforcement requirements or on the basis of domestic US legislation. The decision therefore enabled interference with the fundamental rights of those persons whose personal data was or could be transferred to the US.[676] It further noted that the decision did not contain any findings on the existence of rules in the US intended to limit such interference, nor on the existence of any effective legal protection against such interference.[677] The CJEU highlighted that the level of protection of fundamental rights and freedoms guaranteed within the EU required legislation interfering with Articles 7 and 8 to lay down clear and precise rules defining the scope and application of a measure, and imposing minimum safeguards, derogations, and limitations regarding the

674 Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215. The Decision was declared invalid by the CJEU in C-632/14, *Maximilian Schrems v. Data Protection Commissioner* [GC].

675 CJEU, C-362/14, *Maximilian Schrems v. Data Protection Commissioner* [GC], 6 October 2015.

676 *Ibid.*, para. 84.

677 *Ibid.*, paras. 88–89.

protection of personal data.[678] Given that the Commission decision did not state that the US in fact ensures such a level of protection by reason of its domestic law or its international commitments, the CJEU concluded that it failed to meet the requirements of the relevant transfer provision in the Data Protection Directive and was therefore invalid.[679]

The US' level of protection was thus not 'essentially equivalent' to the fundamental rights and freedoms guaranteed by the EU.[680] The CJEU argued that various articles of the EU Charter of Fundamental Rights were violated. Firstly, the essence of Article 7 was compromised, as US legislation was "permitting the public authorities to have access on a generalised basis to the content of electronic communications". Secondly, the essence of Article 47 was also violated, as the legislation did not provide individuals with legal remedies concerning access to personal data or rectification or erasure of personal data. Lastly, given that the Safe Harbour arrangement violated the above articles, personal data were no longer lawfully processed, resulting in a violation of Article 8.

After the CJEU declared the Safe Harbour arrangement invalid, the Commission and the US agreed on a new framework, the EU-US Privacy Shield. On 12 July 2016, the Commission adopted a decision declaring that the US ensures an adequate level of protection for personal data transferred from the Union to organisations in the US under the Privacy Shield.[681]

Similarly to the Safe Harbour arrangement, the EU-US Privacy Shield framework aims to protect personal data that are transferred from the EU to the US for commercial purposes.[682] US companies can voluntarily self-certify their adherence to the

678 *Ibid.*, paras. 91–92.

679 *Ibid.*, paras. 96–97.

680 *Ibid.*, paras. 73–74 and 96.

681 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207. The Article 29 Working Party welcomed the improvements brought by the Privacy Shield mechanism compared to the Safe Harbour decision and commended the Commission and the US authorities for having taken into consideration in the final version of the Privacy Shield documents the concerns voiced in their opinion WP238 on the draft EU-U.S. Privacy Shield adequacy decision. Nevertheless, it highlighted a number of outstanding concerns. For more details, see Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision*, adopted on 13 April 2016, 16/EN WP 238.

682 For more information, see the EU-U.S. Privacy Shield factsheet.

Privacy Shield list by committing to meet the framework's data protection standards. The competent US authorities monitor and verify the compliance of the certified companies with these standards.

In particular, the Privacy Shield scheme provides for:

- data protection obligations on companies receiving personal data from the EU;
- protection and redress for individuals, in particular the establishment of an ombudsperson mechanism, which is independent from the US intelligence services and deals with complaints from individuals who believe their personal data have been used in an unlawful way by the US authorities in the area of national security;
- an annual joint review to monitor the framework's implementation;[683] the first review took place in September 2017.[684]

The US government has written commitments and assurances that accompany the Privacy Shield decision. These provide limitations and safeguards for the US government's access to personal data for law enforcement and national security purposes.

7.3.2. Transfers subject to appropriate safeguards

Both **EU law** and **CoE law** recognise appropriate safeguards between the data-exporting controller and the recipient in the third country or international organisation as being a possible means of ensuring a sufficient level of data protection for the recipient.

Under **EU law**, personal data transfers to a third country or to an international organisation are allowed if the controller or processor provides appropriate safeguards and enforceable rights, and if effective legal remedies are available to data subjects.[685] The list of acceptable 'appropriate safeguards' is provided exclusively in EU data protection law. Appropriate safeguards can be established by:

683 For more information, see the European Commission web page on the EU-U.S. Privacy Shield.

684 European Commission, Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield, COM(2017) 611 final, 18 October 2017.

685 General Data Protection Regulation, Art. 46.

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules;
- standard data protection clauses adopted either by the European Commission or by a supervisory authority;
- codes of conduct;
- certification mechanisms.[686]

Customised contractual clauses between the controller or processor in the EU and the data recipient in a third country are another means of providing appropriate safeguards. Such contractual clauses, however, need to be authorised by the competent supervisory authority before they can be relied upon as a tool for the transfer of personal data. Similarly, public authorities can make use of data protection provisions included in their administrative arrangements, provided that the supervisory authority has authorised these.[687]

Under CoE law, data flows to a state or international organisation that is not a party to the Modernised Convention 108 are allowed, provided that an appropriate level of protection is secured. This can be achieved by:

- the law of the state or an international organisation; or
- ad hoc or standardised safeguards embedded in a legally binding document.[688]

Transfers subject to contractual clauses

Both **CoE law** and **EU law** recognise contractual clauses between the data-exporting controller and the recipient in the third country as being a possible means of safeguarding a sufficient level of data protection for the recipient.[689]

686 General Data Protection Regulation, Art. 46 (1) (c), (d), (2) (a), (b), (e), (f) and 47.

687 *Ibid*., Art. 46 (3).

688 Modernised Convention 108, Art. 14 (3) (b).

689 General Data Protection Directive, Art. 46 (3); Modernised Convention 108, Art. 14(3)(b).

At the **EU level**, the European Commission with the assistance of the Article 29 Working Party developed standard data protection clauses which were officially certified by a Commission decision as proof of adequate data protection.[690] As Commission decisions are binding in their entirety in the Member States, the national authorities that supervise data transfers must acknowledge these standard contractual clauses in their procedures.[691] Thus, if the data-exporting controller and the third-country recipient agree and sign these clauses, this ought to provide the supervisory authority with sufficient proof that adequate safeguards are in place. Yet in the *Schrems* case, the CJEU held that the European Commission does not have the competence to restrict the powers of the national supervisory authorities to oversee the transfer of personal data to a third country which has been the subject of a Commission adequacy decision.[692] Thus, national supervisory authorities are not prevented from exercising their powers, including the power to suspend or ban a transfer of personal data when the transfer is carried out in violation of EU or national data protection law, such as, for instance, when the data importer does not respect the standard contractual clauses.[693]

The existence of standard data protection clauses in the EU legal framework does not prevent controllers from formulating other ad hoc, individual contractual clauses, as long as the supervisory authority has approved these clauses.[694] They would, however, have to ensure the same level of protection as provided by the standard data protection clauses. When approving ad hoc clauses, supervisory authorities are required to apply the consistency mechanism, so as to ensure a consistent regulatory approach across the EU.[695] This means that the competent supervisory authority has to communicate its draft decision on the clauses to the EDPB. The EDPB will issue an opinion on the matter, and the supervisory authority must take utmost account of this opinion in proceeding with its decision. If it does not intend to follow

690 *Ibid.*, Art. 46 (2) (b) and Art. 46 (5).

691 *Ibid.*, Art. 46 (3); Ad hoc Committee on Data Protection (CAHDATA), Explanatory Report of the Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, para. 105.

692 CJEU, C-362/14, *Maximilian Schrems v. Data Protection Commissioner* [GC], 6 October 2015, paras. 96–98 and 102–105.

693 In order to take account of the CJEU's stance in the *Schrems* case, the Commission amended its Decision on standard contractual clauses. Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council, OJ 2016 L344.

694 General Data Protection Regulation, Art. 46 (3) (a).

695 *Ibid.*, Art. 63 and Art. 64 (1) (e).

the EDPB opinion, the dispute resolution mechanism within the EDPB will be triggered and the Board will adopt a binding decision.[696]

The most important features of a standard contractual clause are:

- a third-party beneficiary clause which enables data subjects to exercise contractual rights even though they are not a party to the contract;
- the data recipient or importer agreeing to be subject to the authority of the data-exporting controller's national supervisory authority and/or courts in the case of a dispute.

There are now two sets of standard clauses available for controller-to-controller transfers from which the data-exporting controller can choose.[697] For controller-to-processor transfers, there is only one set of standard contractual clauses.[698] However, these standard contractual clauses are currently the subject of legal proceedings.

Example: After the CJEU declared the Safe Harbour Decision invalid,[699] personal data transfers to the US could no longer be based on that adequacy decision. While negotiations with the US authorities were ongoing, and pending the adoption of a new adequacy decision (eventually adopted on 12 July 2016),[700] transfers could only be carried out under other legal bases, such as standard contractual clauses or binding corporate rules. Several companies, including Facebook Ireland (against which the case that led to

696 *Ibid.*, Art. 64 and Art. 65.

697 Set I is contained in the Annex to the European Commission (2001), Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, OJ 2001 L 181; Set II is contained in the Annex to European Commission (2004), Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ 2004 L 385.

698 European Commission (2010), Commission Decision 2010/87 of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ 2010 L 39. At the time of the drafting of the handbook, the use of standard contractual clauses as a basis for transfers of personal data to the US was subject to legal proceedings before the Irish High Court.

699 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 6 October 2015.

700 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207.

the invalidation of the Safe Harbour Decision was brought), switched to standard contractual clauses to continue their EU-US data transfers.

Mr Schrems submitted a complaint to the Irish supervisory authority, requesting it to suspend data transfers to the US on the basis of standard contractual clauses. In essence, he claimed that when his personal data are transferred from Facebook's Irish subsidiary to Facebook Inc., and to servers located in the US, there was no guarantee that it would be protected. Facebook Inc. is bound by American laws that could oblige it to disclose personal data to US law enforcement authorities and there is no judicial remedy available for European individuals to contest this practice.[701] For these reasons, the CJEU concluded that the Safe Harbour Decision was invalid, and while the court's judgment was limited to examining that decision, the applicant considered the issues raised to be as pertinent when the transfer is based on contractual clauses. At the time of writing, the case was being examined before the Irish High Court. The applicant apparently intends to take the case to the CJEU, where his aim is to challenge the validity of the European Commission's decision on standard contractual clauses. As described in Chapter 5, only the CJEU has competence to declare an EU instrument invalid.

Transfers subject to binding corporate rules

EU law also allows for personal data transfers based on binding corporate rules for international transfers that take place within the same group of enterprises or undertakings that are part of a joint economic activity.[702] Before binding corporate rules can be relied upon as a tool for the transfer of personal data, the competent supervisory authority needs to approve them, in accordance with binding corporate rules, making use of the consistency mechanism.

In order to be approved, binding corporate rules need to be legally binding, cover all the essential data protection principles and apply to – and be enforced by – every member of the group. They must expressly confer enforceable rights on data subjects, include all essential data protection principles and comply with certain formal requirements, such as stating the structure of the undertaking, describing the

701 For more information, see the revised complaint of the Irish Data Protection Commissioner against Facebook Ireland Ltd and Maximilian Schrems on 1 December 2015.

702 General Data Protection Regulation, Art. 47.

transfers and how data protection principles will be applied. This includes providing such information to data subjects. Binding corporate rules must specify, amongst other things, data subjects' rights and provisions on liability for any breach of the rules.[703] When approving binding corporate rules, the consistency mechanism for the cooperation of the supervisory authorities (described in Chapter 5) will be triggered.

In the framework of the consistency mechanism, the lead supervisory authority reviews the proposed binding corporate rules, adopts a draft decision and communicates it to the EDPB. The Board issues an opinion on the matter, and the lead supervisory authority can formally approve the binding corporate rules whilst taking 'utmost account' of the Board's opinion. This opinion is not legally binding, but if the supervisory authority intends to disregard the opinion, then the dispute resolution mechanism is triggered and the Board will need be called to adopt a legally binding decision, by a two-thirds majority of its members.[704]

Under **CoE law**, the ad hoc or standardised safeguards, which are embedded in a legally binding document,[705] also include binding corporate rules.

7.3.3. Derogations for specific situations

Under EU law, personal data transfers to a third country may be justified, even in the absence of an adequate decision or safeguards, such as standard contractual clauses or binding corporate rules, in any of the following circumstances:

- the data subject gives explicit consent for the data transfer;
- the data subject enters – or is preparing to enter – into a contractual relationship where the transfer of data abroad is necessary;
- to conclude a contract between a data controller and a third party in the interests of the data subject;
- for important reasons of public interest;
- to establish, exercise or defend legal claims;

703 For a more detailed description, see General Data Protection Regulation, Art. 47.

704 *Ibid*., Art. 57 (1) (s), 58 (1) (j), 64 (1) (f), 65 (1) and (2).

705 Modernised Convention 108, Art. 14 (3) (b).

- to protect the vital interests of the data subject;

- for the transfer of data from public registers (this is an instance of prevailing interests of the general public to be able to access information stored in public registers).[706]

Where none of these conditions applies, and where the transfers cannot be based on an adequacy decision or appropriate safeguards, a transfer may take place only when it is not repetitive, concerns a limited number of data subjects and is necessary for the purposes of the data controller's compelling legitimate interests, provided that the data subject's rights do not override these.[707] In these cases, the controller needs to assess the circumstances surrounding the transfer and to provide safeguards. It must also inform the supervisory authority and the data subjects affected of both the transfer and the legitimate interest justifying it.

The fact that derogations are a last resort for lawful transfers[708] (to be used only in the absence of an adequacy decision and if no other safeguards are in place) emphasises their exceptional nature, and is further highlighted in the GDPR's recitals. As such, derogations are accepted as a possibility "for transfers in certain circumstances" on the basis of consent, and where "the transfer is occasional and necessary"[709] in relation to a contract or a legal claim.

Additionally, according to guidance from the Article 29 Working Party, relying on derogations for specific situations must be exceptional, based on individual cases, and cannot be used for massive or repetitive transfers.[710] The European Data Protection Supervisor also underlined the exceptional character of derogations used as legal basis for transfers under Regulation 45/2001, noting that this solution should be used 'in limited cases' and 'for occasional transfers'.[711]

706 General Data Protection Regulation, Art. 49.

707 *Ibid.*

708 *Ibid.*, Art. 49 (1).

709 *Ibid.*

710 Article 29 Working Party (2005), *Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995*, WP 114, Brussels, 25 November 2005.

711 European Data Protection Supervisor, *The transfer of personal data to third countries and international organisations by EU institutions and bodies*, Position Paper, Brussels, 14 July 2014, p. 15.

Example: A Global Distribution System (GDS) service company, with headquarters in the US, provides the online reservations system for multiple airlines, hotels and cruises all over the world, processing data of tens of millions of persons in the EU. For initially transferring data to their servers in the US, the GDS company relies on a derogation as a lawful basis for transfers, this being the necessity to enter a contract. Thus, it is not adducing any other safeguards for the personal data originating in Europe, transferred to the US and then redistributed to hotels all over the world (meaning no safeguards for onward transfers either). The GDS company is not complying with the GDPR requirements for lawful international data transfers, because it relies on a derogation as a lawful ground for massive transfers.

Unless an adequacy decision is in place, the EU or its Member States are empowered to set limits on the transfer of specific categories of personal data to a third country, despite other conditions for such transfers being met, for important reasons of public interest. These limits ought to be perceived as exceptional, and Member States are required to communicate the relevant provisions to the Commission.[712]

CoE law allows for data flows to territories that do not have appropriate data protection in cases where:

- the data subject has given consent;
- the interests of the data subject require it;
- there are prevailing legitimate interests, in particular important public interests, provided for by law;
- it constitutes a necessary and proportionate measure in a democratic society.[713]

7.3.4. Transfers based on international agreements

The EU may conclude international agreements with third countries regulating the transfer of personal data for specific purposes. Those agreements must include appropriate safeguards to ensure the protection of the personal data of the

712 See especially Article 29 Working Party (2005), *Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995*, WP 114, Brussels, 25 November 2005.

713 Modernised Convention 108, Art. 14 (4).

individuals in question. The GDPR exists without prejudice to these international agreements.[714]

Member States may also conclude international agreements with third countries or international organisations that provide an appropriate level of protection of the fundamental rights and freedoms of individuals, insofar as those agreements do not affect the application of the GDPR.

A similar rule is provided in Article 12 (3) (a) of Modernised Convention 108.

Examples of international agreements involving the transfer of personal data are the passenger name records (PNR) agreements.

Passenger Name Records

PNR data are collected by air carriers during the flight reservation process and include, among others, the names, addresses, credit card details and seat numbers of air passengers. Air carriers also collect this information for their own commercial purposes. The EU has entered into agreements with certain third countries (Australia, Canada and the US) for the transfer of PNR data to prevent, detect, investigate and prosecute terrorist offences or serious transnational crime. In addition, the Union adopted Directive (EU) 2016/861 – known as the EU-PNR Directive[715] – in 2016. This directive provides a legal framework for EU Member States to transfer PNR data to competent authorities in other third countries, to similarly prevent, detect, investigate or prosecute terrorist offences and serious crimes. PNR transfers to third country authorities are on a case-by-case basis and are subject to an individual assessment on whether the transfer is necessary for the purposes specified in the directive and provided that fundamental rights are respected.

Concerning PNR agreements between the EU and third countries, their compatibility with the fundamental rights to privacy and data protection enshrined in the EU Charter of Fundamental Rights has been contested. When – following negotiations with Canada – the EU signed an agreement on the transfer and processing of PNR data in 2014, the European Parliament decided to refer the matter to the CJEU to assess the

714 General Data Protection Regulation, Recital 102.

715 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ 2016 L 119.

legality of the agreement with EU law, and in particular with Articles 7 and 8 of the Charter.

Example: In its Opinion on the legality of the EU-Canada PNR agreement,[716] the CJEU held that in its current form, the envisaged agreement was incompatible with the fundamental rights recognised by the Charter, and therefore, could not be concluded. Since it involved personal data processing, it constituted an interference with the right to protection of personal data protected under Article 8 of the Charter. At the same time, it also represents a limitation of the right to respect for private life, enshrined in Article 7, given that taken as a whole, PNR data may be aggregated and analysed in a way which reveals travel habits, relationships between different individuals, information about their financial situation, dietary habits and health situation, thus impinging on their private lives.

The interference with the fundamental rights that the envisaged agreement brought pursued an objective of general interest, namely public security and the fight against terrorism and serious transnational crime. However, the CJEU recalled that to be justified, an interference must be limited to what is strictly necessary to achieve the pursued aim. After analysing its provisions, the CJEU concluded that the envisaged agreement did not meet the 'strict necessity' criterion. Among the factors that the CJEU considered to reach that conclusion were the following:

- The fact that the envisaged agreement entailed the transfer of sensitive data. The PNR collected pursuant to the envisaged agreement could include sensitive data, such as information revealing racial or ethnic origin, religious beliefs or the health status of a passenger. The transfer and processing of sensitive data by the Canadian authorities could present a risk to the principle of non-discrimination, and thus required a precise and solid justification, based on grounds other than public security and the fight against serious crime. The envisaged agreement failed to provide such justification.[717]

716 CJEU, *Opinion 1/15 of the Court (Grand Chamber)*, 26 July 2017.

717 *Ibid*., para. 165.

- The continued storage of the PNR data of all passengers, for a period of five years, even after passengers departed from Canada was also considered to exceed the limits of strict necessity. The CJEU considered that it would be permissible for Canadian authorities to retain the data of passengers whom objective evidence suggests may present a threat to public security, even after those persons have departed from Canada. By contrast, the storage of personal data of *all* passengers, for whom there is not even indirect evidence presenting them as a risk to public security, is not justified.[718]

The Consultative Committee of Convention 108 has provided an opinion on the data protection implications of PNR agreements under CoE law.[719]

Messaging data

The Belgium-based Society for Worldwide Interbank Financial Telecommunication (SWIFT), which is the processor for most of the global money transfers from European banks, operated with a 'mirror' centre in the US and was confronted with a request to disclose data to the US Department of the Treasury for terrorism investigation purposes under its Terrorist Finance Tracking Programme.[720]

From the EU perspective, there was no sufficient legal basis for disclosing these data – mainly about citizens in the EU – to the US simply on the grounds that only because one of SWIFT's data service-processing centres were located there.

A special agreement between the EU and the US, known as the SWIFT Agreement, was concluded in 2010 to provide the necessary legal basis and to ensure adequate data protection standards.[721]

718 *Ibid.*, paras. 204–207.

719 Council of Europe, *Opinion on the Data protection implications of the processing of Passenger Name Records*, T-PD(2016)18rev, 19 August 2016.

720 See, in this context, Article 29 Working Party (2011), *Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing*, WP 186, Brussels, 13 June 2011; Article 29 Working Party (2006), *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT)*, WP 128, Brussels, 22 November 2006; Belgium Commission for the protection of privacy (*Commission de la protection de la vie privée*) (2008), *'Control and recommendation procedure initiated with respect to the company SWIFT scrl'*, Decision, 9 December 2008.

721 Council Decision 2010/412/EU of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ 2010 L 195, pp. 3 and 4. The text of the Agreement is attached to this Decision, OJ 2010 L 195, pp. 5–14.

Under this agreement, financial data stored by SWIFT continue to be provided to the US Treasury Department for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing. The US Treasury Department may request financial data from SWIFT, provided that the request:

- identifies as clearly as possible the financial data;
- clearly substantiates the necessity of the data;
- is tailored as narrowly as possible to minimise the amount of data requested;
- does not seek any data relating to the Single Euro Payments Area (SEPA).[722]

Europol must receive a copy of each request made by the US Treasury Department and verify whether or not the principles of the SWIFT Agreement are being complied with.[723] If it is confirmed that they are, SWIFT must provide the financial data directly to the US Treasury Department. The department must store the financial data in a secure physical environment where they are accessed only by analysts investigating terrorism or its financing, and the financial data must not be interconnected with any other database. In general, financial data received from SWIFT must be deleted no later than five years from its receipt. Financial data which are relevant to specific investigations or prosecutions may be retained only for as long as the data are necessary for these investigations or prosecutions.

The US Treasury Department may transfer information from the data received by SWIFT to specific law enforcement, public security or counter-terrorism authorities within or outside the US exclusively for the investigation, detection, prevention or prosecution of terrorism and its financing. Where the onward transfer of financial data involves a citizen or resident of an EU Member State, any sharing of the data with the authorities of a third country is subject to the prior consent of the competent authorities of the concerned Member State. Exceptions may be made where the sharing of the data is essential for the prevention of an immediate and serious threat to public security.

Independent overseers, including a person appointed by the European Commission, monitor compliance with the principles of the SWIFT Agreement. They have

722 *Ibid.*, Art. 4 (2).

723 The Joint Supervisory Body of Europol has conducted audits on Europol's activities in this area.

the possibility to review in real time and retroactively all searches made of the provided data, to request additional information to justify the terrorism nexus of these searches, and the authority to block any or all searches that appear to be in breach of the safeguards laid down in the agreement.

Data subjects have a right to obtain confirmation from the competent EU supervisory authority that their personal data protection rights have been complied with. Data subjects also have the right to the rectification, erasure or blocking of their data that has been collected and stored by the US Treasury Department under the SWIFT Agreement. However, the access rights of data subjects may be subject to certain legal limitations. Where access is refused, the data subject must be informed in writing of the refusal and of their right to seek administrative and judicial redress in the US.

The SWIFT Agreement is valid for five years, its first period of validity lasted until August 2015. It automatically extends for subsequent periods of one year unless one of the parties notifies the other, at least six months in advance, of its intention not to extend the agreement. The automatic prolonging has been applied in August 2015, 2016 and 2017 and ensures the validity of the SWIFT Agreement until at least August 2018.[724]

724 *Ibid.*; Art. 23 (2).

8

Data protection in the context of police and criminal justice

EU	Issues covered	CoE
Data Protection Directive for Police and Criminal Justice Authorities	**In general**	Modernised Convention 108
	Police	Police Recommendation Practical Guide on the use of personal data in the police sector
	Surveillance	ECtHR, *B.B. v. France*, No. 5335/06, 2009 ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 2008 ECtHR, *Allan v. the United Kingdom*, No. 48539/99, 2002 ECtHR, *Malone v. the United Kingdom*, No. 8691/79, 1984 ECtHR, *Klass and Others v. Germany*, No. 5029/71, 1978 ECtHR, *Szabó and Vissy v. Hungary*, No. 37138/14, 2016 ECtHR, *Vetter v. France*, No. 59842/00, 2005
	Cybercrime	Cybercrime Convention

EU	Issues covered	CoE
Other specific legal instruments		
Prüm Decision	For special data: fingerprints, DNA, hooliganism, air passenger information, telecommunications' data etc.	Modernised Convention 108, Article 6 Police Recommendation, Practical Guide on the use of personal data in the police sector
Swedish Initiative (Council Framework Decision 2006/960/JHA)	Simplifying the exchange of information and intelligence between law enforcement authorities	ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 2008
Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Kärntner Landesregierung and Others* [GC], 2014 CJEU, Joined cases C-203/15 and C-698/15, *Tele2 Sverige and Home Department v. Tom Watson and Others* [GC], 2016	Retention of personal data	ECtHR, *B.B. v. France*, No. 5335/06, 2009
Europol Regulation Eurojust Decision	By special agencies	Police Recommendation
Schengen II Decision VIS Regulation Eurodac Regulation CIS Decision	By special joint information systems	Police Recommendation ECtHR, *Dalea v. France*, No. 964/07, 2010

In order to balance the individual's interests in data protection and society's interests in data collection for the sake of fighting crime and ensuring national and public safety, the CoE and the EU have enacted specific legal instruments. This section provides an overview of CoE (Section 8.1) and EU law (Section 8.2) in relation to data protection in police and criminal justice matters.

8.1. CoE law on data protection and national security, police and criminal justice matters

Key points

- The Modernised Convention 108 and the CoE Police Recommendation apply to data protection across all areas of police work.
- The Cybercrime Convention (Budapest Convention) is a binding international legal instrument dealing with crimes committed against, and by means of, electronic networks. It is also relevant for the investigation of non-cyber-crimes that involve electronic evidence.

One important distinction between CoE and EU law is that **CoE law**, unlike EU law, also applies to the national security area. This means that Contracting Parties need to stay within the remit of Article 8 of the ECHR even for activities related to national security. Several of the ECtHR's judgments concern state activities in the sensitive areas of national security law and practice.[725]

Concerning police and criminal justice, at the European level, Modernised Convention 108 covers all fields of the processing of personal data, and its provisions are intended to regulate the processing of personal data in general. Consequently, Modernised Convention 108 applies to data protection in the area of police and criminal justice. The processing of genetic data, personal data relating to offences, criminal proceedings and convictions and any related security measures, biometric data that uniquely identify a person, as well as any sensitive personal data, is only allowed where appropriate safeguards exist against the risks that the processing of such data may pose to the interests, rights and fundamental freedoms of the data subject; notably, the risk of discrimination.[726]

The legal tasks of police and criminal justice authorities often require the processing of personal data, which may have serious consequences for the individuals concerned. The Police Recommendation adopted by the CoE in 1987 gives guidance to the CoE member states on how they should give effect to the principles

725 See, for example, ECtHR, *Klass and Others v. Germany*, No. 5029/71, 6 September 1978; ECtHR, *Rotaru v. Romania* [GC], No. 28341/95, 4 May 2000 and ECtHR, *Szabó and Vissy v. Hungary*, No. 37138/14, 12 January 2016.

726 Modernised Convention 108, Art. 6.

of Convention 108 in the context of personal data processing by police authorities.[727] The Recommendation was complemented by a practical guide on the use of personal data in the police sector, adopted by the Consultative Committee of Convention 108.[728]

Example: In *D.L. v. Bulgaria*,[729] social services placed the applicant in a secure educational institution pursuant to a court order. All written correspondence and telephone conversations were subject to blanket and indiscriminate surveillance by the institution. The ECtHR held that Article 8 had been violated, given that the measure in question was not necessary in a democratic society. The Court stated everything had to be done to enable minors placed in an institution to have sufficient contact with the outside world, as this was an integral part of their right to be treated with dignity, and was absolutely essential in preparing their reintegration into society. This applied as much to visits as to written correspondence or telephone conversations. Furthermore, the surveillance did not make any distinction between communication with family members and NGOs representing children's rights or lawyers. Moreover, the decision to intercept the communication was not based on an individualised analysis of the risks in each particular case.

Example: In *Dragojević v. Croatia*,[730] the applicant was suspected of being involved in drug-trafficking. He was found guilty after an investigating judge authorised the use of secret surveillance measures to intercept the applicant's telephone calls. The ECtHR held that the measure, against which a complaint was raised, constituted an interference with the right to respect for private life and correspondence. The authorisation given by the investigating judge was based merely on the prosecuting authority's statement that "the investigation could not be conducted by other means". The ECtHR also noted that the criminal courts had limited their assessment regarding the use of the surveillance measures, and that the government did not put forward the remedies that are available. Consequently, Article 8 had been violated.

727 Council of Europe, Committee of Ministers (1987), Recommendation Rec(87)15 to member states regulating the use of personal data in the police sector, 17 September 1987.

728 Council of Europe (2018), Consultative Committee of Convention 108, Practical Guide on the use of personal data in the police sector, T-PD(2018)1.

729 ECtHR, *D.L. v. Bulgaria*, No. 7472/14, 19 May 2016.

730 ECtHR, *Dragojević v. Croatia*, No. 68955/11, 15 January 2015.

8.1.1. The police recommendation

The ECtHR has consistently held that the storing and retention of personal data by police or national security authorities constitutes an interference with Article 8 (1) of the ECHR. Many ECtHR judgments deal with the justification of such interference.[731]

Example: In *B.B. v. France*,[732] the applicant was sentenced for engaging in sex offences against 15-year-old minors as a person in a position of trust. He completed his prison sentence in 2000. A year later, he requested that the mention of this sentence be removed from his criminal record, but the request was rejected. In 2004, a French law established a national judicial database of sex offenders and the applicant was informed of his inclusion therein. The ECtHR held that including a convicted sex offender in a national judicial database fell under Article 8 of the ECHR. However, given that sufficient data protection safeguards had been implemented, such as the data subject's right to request erasure of the data, the limited length of data storage and the restricted access to such data, a fair balance had been struck between the competing private and public interests at stake. The Court concluded that there had not been a violation of Article 8 of the ECHR.

Example: In *S. and Marper v. the United Kingdom*,[733] both applicants had been charged with, but not convicted of, criminal offences. Nonetheless, their fingerprints, cellular samples and DNA profiles were kept and stored by the police. The unlimited retention of the aforementioned biometric data was permitted by statute where a person was suspected of a criminal offence, even if the suspect was later acquitted or discharged. The ECtHR held that the blanket and indiscriminate retention of personal data, which was not time-limited and where acquitted individuals had only limited possibilities to request deletion, constituted a disproportionate interference with the applicants' right to respect for private life. The Court concluded that there had been a violation of Article 8 of the ECHR.

731 See, for example, ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987; ECtHR, *M.M. v. the United Kingdom*, No. 24029/07, 13 November 2012; ECtHR, *M.K. v. France*, No. 19522/09, 18 April 2013, or ECtHR, *Aycaguer v. France*, No. 8806/12, 22 June 2017.

732 ECtHR, *B.B. v. France*, No. 5335/06, 17 December 2009.

733 ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008, paras. 119 and 125.

A crucial issue in the context of electronic communications is the interference by public authorities with the rights to privacy and data protection. Means of surveillance or interception of communications, such as listening or tapping devices, are permissible only if this is provided for by law and if it constitutes a necessary measure in a democratic society in the interests of:

- protecting state security;
- public safety;
- the monetary interests of the state;
- the suppression of criminal offences; or
- protecting the data subject or the rights and freedoms of others.

Many further ECtHR judgments deal with the justification of interference with the right to privacy through carrying out surveillance.

Example: In *Allan v. the United Kingdom*,[734] the authorities secretly recorded private conversations between a prisoner and a friend in the visiting area of the prison and with a co-accused in a prison cell. The ECtHR held that the use of the audio- and video-recording devices in the applicant's cell, the prison visiting area and on a fellow prisoner amounted to an interference with the applicant's right to private life. Since there was no statutory system to regulate the use of covert recording devices by the police at the relevant time, this interference was not in accordance with the law. The Court concluded that there had been a violation of Article 8 of the ECHR.

Example: In *Roman Zakharov v. Russia*,[735] the applicant brought judicial proceedings against three mobile network operators. He argued that his right to the privacy of his telephone communications had been violated, as the operators had installed equipment allowing the Federal Security Service to intercept his telephone communications without prior judicial authorisation. The ECtHR held that the domestic legal provisions governing the interception of communications did not provide adequate and effective

734 ECtHR, *Allan v. the United Kingdom*, No. 48539/99, 5 November 2002.

735 ECtHR, *Roman Zakharov v. Russia*, No. 47143/06, 4 December 2015.

guarantees against arbitrariness and the risk of abuse. In particular, national law did not require deleting the stored data after the purpose of storage had been achieved. Furthermore, even though judicial authorisation was required, judicial scrutiny was limited.

Example: In *Szabó and Vissy v. Hungary*,[736] the applicants claimed that Hungarian legislation violated Article 8 of the ECHR, as it was not sufficiently detailed or precise. Furthermore, it was argued that the legislation did not provide sufficient guarantees against abuse and arbitrariness. The ECtHR held that Hungarian law did not require surveillance to be subject to authorisation by a court. Nevertheless, the Court noted that while it was subjected to the approval of the Minister of Justice, this supervision was eminently political and incapable of ensuring the required assessment of 'strict necessity'. Furthermore, the national law did not provide for judicial review, given that no notification would be sent to the subjects. The Court concluded that there had been a violation of Article 8 of the ECHR.

As data processing by police authorities may have a significant impact on the persons concerned, detailed data protection rules for the processing of personal data in this area are especially necessary. The CoE Police Recommendation sought to address this issue by giving guidance on how personal data should be collected for police work; how data files in this area should be kept; who should be allowed to access these files, including the conditions for transferring personal data to foreign police authorities; how data subjects should be able to exercise their data protection rights; and how control by independent authorities should be implemented. The obligation to provide adequate data security was also considered.

The recommendation does not provide for the open-ended, indiscriminate collection of personal data by police authorities. It limits the collection of personal data by police authorities to that which is necessary for the prevention of a real danger or the prosecution of a specific criminal offence. Any additional data collection would have to be based on specific national legislation. Processing of sensitive data should be limited to that which is absolutely necessary in the context of a particular inquiry.

Where personal data are collected without the knowledge of the data subject, the data subject has to be informed of the data collection as soon as such disclosure no longer prejudices an investigation. The collection of data by technical surveillance or other automated means must have a specific legal basis.

736 ECtHR, *Szabó and Vissy v. Hungary*, No. 37138/14, 12 January 2016.

Example: In *Versini-Campinchi and Crasnianski v. France,*[737] the applicant, a lawyer, had a telephone conversation with a client whose telephone line was being intercepted at the request of an investigating judge. The transcript of the conversation showed that she had disclosed information covered by legal professional privilege. The prosecutor sent this information to the Bar Council, which imposed a penalty on the applicant. The ECtHR acknowledged the existence of an interference with the right to respect for private life and correspondence, not only of the person whose telephone had been tapped, but also of the applicant whose communication had been intercepted and transcribed. The interference had been made in accordance with the law and pursued the legitimate aim of the prevention of disorder. The applicant had obtained a review of the lawfulness of the submission of the transcript of the telephone-tapping records in the context of the disciplinary proceedings brought against her. Even though she had not been able to apply to have the transcript of the telephone conversation annulled, the ECtHR considered that there had been effective scrutiny capable of limiting the interference complained of to that which was necessary in a democratic society. The ECtHR held that the argument that the possibility of criminal proceedings against a lawyer on the basis of the transcript could have a chilling effect on the freedom of communication between a lawyer and his or her client, and thus on the latter's defence rights, was not credible where the disclosure made by the lawyer herself were capable of amounting to illegal conduct on her part. Consequently, no violation of Article 8 was found.

The CoE Police Recommendation provides that, when storing personal data, clear distinctions must be made between: administrative data and police data; the personal data of different types of data subjects, such as suspects, convicted persons, victims and witnesses; and data considered to be hard facts and those based on suspicions or speculation.

The purpose for which police data may be used must be strictly limited. This has consequences for the disclosure of police data to third parties: the transfer or disclosure of such data within the police sector should be governed by whether or not there is a legitimate interest in sharing the information. The transfer or disclosure of such data outside the police sector should be allowed only where there is a clear legal obligation or authorisation.

737 ECtHR, *Versini-Campinchi and Crasnianski v. France*, No. 49176/11, 16 June 2016.

Example: In *Karabeyoğlu v. Turkey*,[738] the applicant, a judge, had his telephone lines monitored in the context of a criminal investigation into an illegal organisation to which he was suspected of belonging, or to which he was thought to provide assistance and support. Following the decision not to prosecute, the public prosecutor in charge of the criminal investigation destroyed the recordings in question. However, a copy had remained in the possession of judicial investigators, who then used the relevant material in the context of a disciplinary investigation against the applicant. The ECtHR held that the relevant legislation had been breached as the information had been used for purposes other than that for which it had been gathered, and had not been destroyed within a statutory time-limit. The interference with the applicant's right to respect for his private life had not been in accordance with the law as far as the disciplinary proceedings against him were concerned.

International transfer or disclosure should be restricted to foreign police authorities and be based on special legal provisions, possibly international agreements, unless it is necessary for the prevention of serious and imminent danger.

Data processing by the police must be subject to independent supervision to ensure compliance with domestic data protection law. Data subjects must have all of the access rights contained within Modernised Convention 108. Where the access rights of data subjects have been restricted according to Article 9 of Convention 108, in the interest of effective police investigations and execution of criminal penalties, the data subject must have the right under domestic law to appeal to the national data protection supervisory authority or to another independent body.

8.1.2. The Budapest Convention on Cybercrime

As criminal activities increasingly use and affect electronic data-processing systems, new criminal legal provisions are needed to meet this challenge. The CoE therefore adopted an international legal instrument – the Convention on Cybercrime, also known as the Budapest Convention – to address the issue of crimes committed against and by means of electronic networks.[739] This convention is also open for accession by non-members of the CoE. As at the beginning of 2018, 14 states

738 ECtHR, *Karabeyoğlu v. Turkey*, No. 30083/10, 7 June 2016.

739 Council of Europe, Committee of Ministers (2001), Convention on Cybercrime, CETS No. 185, Budapest, 23 November 2001, entered into force on 1 July 2004.

outside the CoE[740] were parties to the convention and seven other non-members have been invited to accede.

The Convention on Cybercrime remains the most influential international treaty dealing with breaches of law over the internet or other information networks. It requires parties to update and harmonise their criminal laws against hacking and other security infringements, including copyright infringement, computer-facilitated fraud, child pornography and other illicit cyber-activities. The convention also provides for procedural powers covering the search of computer networks and the interception of communications in the context of fighting cybercrime. Finally, it enables effective international cooperation. An additional protocol to the convention deals with the criminalisation of racist and xenophobic propaganda in computer networks.

While the convention is not an instrument aimed at promoting data protection, it criminalises activities that are likely to violate a data subject's right to the protection of his or her data. Furthermore, it requires Contracting Parties to adopt legislative measures to enable their national authorities to intercept traffic and content data.[741] It also obliges the Contracting Parties, when implementing the convention, to foresee adequate protection of human rights and liberties, including the rights guaranteed under the ECHR, such as the right to data protection.[742] Contracting parties are not required to also join Convention 108 in order to join the Budapest Convention on Cybercrime.

8.2. EU law on data protection in police and criminal justice matters

Key points

- Within the EU, data protection in the police and criminal justice sector is regulated in the context of both national and cross-border processing by police and criminal justice authorities of the Member States and EU actors.
- At the Member State level, the Data Protection Directive for Police and Criminal Justice Authorities needs to be incorporated into national law.

740 Australia, Canada, Chile, the Dominican Republic, Israel, Japan, Mauritius, Panama, Senegal, Sri Lanka, Tonga and the United States. See Chart of signatures and ratifications of Treaty 185, status as of July 2017.

741 Council of Europe, Committee of Ministers (2001), Convention on Cybercrime, CETS No. 185, Budapest, 23 November 2001, Art. 20 and 21.

742 *Ibid.,* Art. 15 (1).

- Specific legal instruments govern data protection in police and law enforcement cross-border cooperation, particularly in combating terrorism and cross-border crime.
- Special data protection rules exist for the European Police Office (Europol), the EU Judicial cooperation unit (Eurojust), and the newly established European Public Prosecutor's Office, which are EU bodies assisting and promoting cross-border law enforcement.
- Special data protection rules also exist for the joint information systems that have been established at the EU level for cross-border information exchanges between the competent police and judicial authorities. Important examples are the Schengen Information System II (SIS II), the Visa Information System (VIS) and Eurodac, a centralised system containing the fingerprint data of third-country nationals and stateless persons applying for asylum in one of the EU Member States.
- The EU is in the process of updating the data protection provisions set out above, so as to be in line with the provisions of the Data Protection Directive for Police and Criminal Justice Authorities.

8.2.1. The Data Protection Directive for Police and Criminal Justice Authorities

Directive 2016/680/EU on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data (the Data Protection Directive for Police and Criminal Justice Authorities)[743] aims to protect personal data collected and processed for criminal justice purposes ranging from:

- prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- executing a criminal penalty; and

743 Directive 2016/680/EU of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119, p. 89 (Data Protection Directive for Police and Criminal Justice Authorities).

- in cases where police or other law-enforcement authorities act to uphold the law and to safeguard against and prevent threats to public security and to the fundamental rights of the society which could constitute a criminal offence.

The Data Protection Directive for Police and Criminal Justice Authorities protects the personal data of different categories of individuals involved in criminal proceedings, such as witnesses, informants, victims, suspects and accomplices. Police and criminal justice authorities are obliged to comply with the directive's provisions whenever they process such personal data for law enforcement purposes, within both the personal and the material scope of the directive.[744]

However, the use of data for a different purpose is also allowed under certain conditions. The processing of data for a different law enforcement purpose than that for which it was collected is only permitted if this is lawful, necessary and proportionate according to national or EU law.[745] For other purposes, the rules of the General Data Protection Regulation apply. The logging and documenting of data sharing is one of the competent authorities' specific duties to assist with the clarification of responsibilities arising from complaints.

Competent authorities working in the area of police and criminal justice are public authorities, or authorities empowered by national law and public powers to perform the functions of a public authority,[746] e.g. privately run prisons.[747] The directive's applicability extends both to data processing at the domestic level and to cross-border processing between Member States' police and judicial authorities, as well as to international transfers by the competent authorities to third countries and international organisations.[748] It does not cover national security or the processing of personal data by the EU institutions, bodies, offices and agencies.[749]

744 Data Protection Directive for Police and Criminal Justice Authorities, Art. 2 (1).

745 *Ibid.*, Art. 4 (2).

746 *Ibid.*, Art. 3 (7).

747 European Commission (2016), Communication from the Commission to the European Parliament pursuant to Article 294 (6) of the Treaty on the Functioning of the European Union concerning the position of the Council on the adoption of a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, COM(2016) 213 final, Brussels, 11 April 2016.

748 Data Protection Directive for Police and Criminal Justice Authorities, Chapter V.

749 *Ibid.*, Art. 2 (3).

The directive relies, to a large extent, on the principles and definitions contained in the General Data Protection Regulation, taking account of the specific nature of the police and criminal justice fields. Supervision may be carried out by the same Member State authorities that exercise it under the General Data Protection Regulation as well. The appointment of Data Protection Officers and the carrying out of Data Protection Impact Assessments have been introduced into the directive as new obligations for police and criminal justice authorities.[750] Although these concepts are inspired by the General Data Protection Regulation, the directive addresses the specific nature of police and criminal justice authorities. Compared to data processing for commercial purposes, which is regulated by the regulation, security-related processing may require some level of flexibility. For instance, providing data subjects with the same level of protection in terms of rights to information, access to, or deletion of their personal data as under the General Data Protection Regulation could mean that any surveillance operation carried out for law enforcement purposes would become ineffective in the context of law enforcement. The directive therefore does not contain the principle of transparency. Similarly, the principles of data minimisation and purpose limitation, requiring that personal data be limited only to what is necessary in relation to the purposes for which they are processed, and to be processed for specified and explicit aims, also need to be applied flexibly in security-related processing. The information collected and stored by competent authorities for a particular case may be found extremely useful in resolving future cases.

Principles relating to processing

The Data Protection Directive for Police and Criminal Justice Authorities sets out some key safeguards regarding the use of personal data. It also spells out the principles guiding the processing of these data. Member States need to ensure that personal data are:

- processed lawfully and fairly;
- collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are processed;

750 *Ibid.*, in Art. 32 and Art. 27, respectively.

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.[751]

Under the directive, processing is lawful only when it occurs to the extent necessary to perform the relevant task. Furthermore, this should be done by a competent authority in pursuit of the objectives specified in the directive and be based on EU or national law.[752] Data must not be kept for longer than is necessary and must be erased or periodically reviewed within certain time-limits. It must only be used by a competent authority and for the purpose for which the data were collected, transmitted or made available.

Rights of the data subject

The directive also sets out the rights of the data subject. These include:

- The right to receive information. Member States must oblige the data controller to make available to the data subject the 1) the identity and contact details of the controller, 2) the contact details of the data protection officer, 3) the purposes of the intended processing, 4) the right to lodge a complaint with the supervisory authority and its contact details and 5) the right to access personal data, to rectify or erase them and to restrict the processing of the data.[753] In addition to these general information requirements, the directive provides that, in specific cases, and to enable the exercise of their rights, controllers must give to the data subjects information about the legal basis for the processing and about how long the data will be stored. If personal data are to be transmitted to other recipients, including in third countries or international organisations,

751 *Ibid.*, Art. 4 (1).

752 *Ibid.*, Art. 8.

753 *Ibid.*, Art. 13 (1).

data subjects must be informed of the categories of such recipients. Finally, controllers must provide any further information, taking the specific circumstances in which the data are processed into account – for example, when personal data were collected during covert surveillance, i.e. without the knowledge of the data subject. This guarantees fair processing in respect of the data subject.[754]

- The right to access personal data. Member States must ensure that the data subject enjoys the right to know whether or not his or her personal data are being processed. If they are, the data subject should have access to certain information, such as the categories of data being processed.[755] However, this right may be restricted – for example, to prevent the obstruction of investigation or prejudicing the prosecution of a crime, or to protect public security and the rights and freedoms of others.[756]

- The right to rectify personal data. Member States are obliged to ensure that a data subject can, without undue delay, obtain the rectification of incorrect personal data. Furthermore, the data subject also has the right to have incomplete personal data completed.[757]

- The right to erase personal data and restrict processing. In certain cases, the controller needs to erase personal data. Furthermore, the data subject may secure the erasure of their personal data, but only when they are being unlawfully processed.[758] In certain situations, the processing of personal data may be restricted rather than erased. This can occur in cases where 1) the accuracy of the personal data has been challenged but this cannot be ascertained or 2) where the personal data are needed for the purpose of evidence.[759]

Whenever the controller refuses to rectify or to erase personal data, or to restrict the processing of the data, the data subject must be informed of this in writing. Member States may restrict this right to information to, amongst other things, protect public

754 *Ibid.*, Art. 13 (2).
755 *Ibid.*, Art. 14.
756 *Ibid.*, Art. 15.
757 *Ibid.*, Art. 16 (1).
758 *Ibid.*, Art. 16 (2).
759 *Ibid.*, Art. 16 (3).

security or the rights and freedoms of others, for the same reasons as for restricting the right to access.[760]

The data subject is normally entitled to information about the processing of his or her personal data, and has the right of access, rectification, or erasure of the restriction of processing, which he or she can exercise directly with the controller. As a fall-back, the indirect exercise of the data subject rights, through its data protection supervisory authority, is also possible under the Police and Criminal Justice Data Protection Directive, and it comes into effect when the controller restricts the right of the data subject.[761] Article 17 of the directive requires that Member States adopt measures ensuring that the rights of data subjects may also be exercised through their supervisory authority. That is why the data controller must inform the data subject of the possibility of indirect access.

Obligations of the controller and processor

In the context of the Data Protection Directive for Police and Criminal Justice Authorities, data controllers are competent public authorities, or other bodies with the relevant public powers and public authority, who determine the purposes and means of the processing of personal data. The directive establishes several obligations for data controllers to ensure a high level of protection for personal data processed for law enforcement purposes.

Competent authorities must keep logs for the processing operations they carry out in automated processing systems. Logs must be kept at least for the collection, alteration, consultation, disclosure including transfers, combination and erasure of the personal data.[762] The directive provides that the logs of consultation and disclosure must make it possible to determine the date and time of the operations, their justification, and as far as possible, the identification of the person who consulted the system or disclosed the personal data, and the recipients of the personal data concerned. The logs must be used only with the aim of verifying the lawfulness of processing, for self-monitoring, for ensuring the integrity and security of the personal data, and for criminal proceedings.[763] On request of the supervisory authority, the controller and processor must make the logs available to it.

760 *Ibid.*, Art. 16 (4).

761 *Ibid.*, Art. 17.

762 *Ibid.*, Art. 25 (1).

763 *Ibid.*, Art. 25 (2).

In particular, there is a general obligation for controllers to implement appropriate technical and organisational measures to ensure that processing is performed in accordance with the directive, and to be able to demonstrate the lawfulness of such processing.[764] When designing those measures, they need to take the nature, scope, context of processing and, importantly, any potential risks to the rights and freedoms of individuals into account. Controllers should adopt internal policies and implement measures that facilitate compliance with the principles of data protection, in particular the principle of data protection by design and by default.[765] Where processing is likely to result in a high risk to the rights of individuals – because of the use of new technologies, for instance – controllers must carry out a data protection impact assessment before commencing the processing.[766] The directive also lists the measures that must be implemented by the controllers to ensure the security of processing. These include measures to prevent unauthorised access to the personal data processed by them, to ensure that authorised persons have access only to the personal data covered by their access authorisation, that the functions of the processing system perform properly, and that stored personal data cannot be corrupted by means of a malfunctioning of the system.[767] If a personal data breach does occur, then controllers must notify the supervisory authority within three days, describing the nature of the breach, its likely consequences, the categories of personal data involved and the approximate number of the respective data subjects affected. The personal data breach must also be communicated to the data subject "without undue delay" where the breach is likely to result in a high risk to his or her rights and freedoms.[768]

The directive contains the principle of accountability, placing a duty on controllers to implement measures to ensure compliance with that principle. Controllers must keep records of all the categories of processing activities under their responsibility: the detailed content of such records is specified in Article 24 of the directive. The records must be made available to the supervisory authority upon request, so that they can monitor the controller's processing operations. Another important measure to enhance accountability is the designation of a Data Protection Officer (DPO). Controllers must designate a DPO, although the directive allows Member States to

764 *Ibid.*, Art. 19.

765 *Ibid.*, Art. 20.

766 *Ibid.*, Art. 27.

767 *Ibid.*, Art. 29.

768 *Ibid.*, Art. 30 and 31.

exempt from that obligation courts and other independent judicial authorities.[769] The duties of the DPO resemble those under the General Data Protection Regulation. He or she monitors compliance with the directive, provides information and advises employees who carry out data processing of their obligations under data protection legislation. The DPO also issues advice about the need to carry out a data protection impact assessment and acts as the contact point for the supervisory authority.

Transfers to third countries or international organisations

Similarly to the General Data Protection Regulation, the directive establishes conditions for the transfer of personal data to third countries or international organisations. If personal data were transmitted freely outside the EU jurisdiction, the safeguards and strong protection provided under EU law could be undermined. However, the conditions themselves are quite different from the ones in the General Data Protection Regulation. The transfer of personal data to third countries or international organisations is allowed if:[770]

- The transfer is necessary for the directive's objectives.
- The personal data are transferred to a competent authority, within the meaning of the directive, of the third country or international organisation – although there is a derogation from this rule in individual and specific cases.[771]
- Transfer to third countries or international organisations of personal data received in the course of cross-border cooperation requires the authorisation of the Member State from which the data originate, although there are exemptions in urgent cases.
- An adequacy decision has been adopted by the European Commission, appropriate safeguards have been established, or the derogation for transfers in specific situations applies.
- Onward transfers of personal data to another third country or an international organisation require the prior authorisation of the originating competent authority, which will take into account, among other things, the seriousness of the

769 *Ibid.*, Art. 32.

770 *Ibid.*, Art. 35.

771 *Ibid*, Art. 39.

offence and the level of data protection in the country of destination of the second international transfer.[772]

Under the directive, transfers of personal data may take place if one of three conditions has been met. The first one is when the European Commission has issued an adequacy decision under the directive. The decision can apply to the whole territory of a third country, or for specific sectors of a third country or for an international organisation. However, this can only be done if an adequate level of protection is ensured and the conditions defined in the directive are met.[773] In such cases, the transfer of personal data is not subject to the authorisation of the Member State.[774] The European Commission has to monitor developments that could affect the functioning of the adequacy decisions. In addition, the decision has to include a mechanism for periodic review. The Commission may also repeal, amend or suspend a decision where available information reveals that the conditions in the third country or international organisation no longer ensure an adequate level of protection. If so, the Commission has to enter into consultations with the third country or international organisation, trying to remedy the situation.

In the absence of an adequacy decision, transfers can be based on appropriate safeguards. They can be laid down in a legally binding instrument or the controller can carry out a self-assessment of the circumstances surrounding the transfer of the personal data and can conclude that appropriate safeguards exist. The self-assessment should take into account possible cooperation agreements concluded between Europol or Eurojust and the third country or international organisation, the existence of confidentiality obligations and the limitation in purpose as well as assurances given that the data will not be used for any form of cruel and inhuman treatment, including the death penalty.[775] In this latter case, the controller needs to inform the competent supervisory authority of the categories of transfers under this category.[776]

Where no adequacy decision has been adopted or no appropriate safeguards have been established, transfers can still be allowed in specific situations outlined in the directive. These include, amongst others, the protection of the vital interests of the

772 *Ibid.*, Art. 35 (1).
773 *Ibid.*, Art. 36.
774 *Ibid.*, Art. 36 (1).
775 *Ibid.*, Recital 71.
776 *Ibid.*, Art. 37 (1).

data subject or another person and the prevention of an immediate and serious threat regarding the public security of the Member State or a third country.[777]

In individual and specific cases, transfers by competent authorities to recipients established in third countries that are not competent authorities may occur if, on top of one of the three conditions described above being met, additional conditions laid down in Article 39 of the directive are met, as well. In particular, the transfer must be strictly necessary for the performance of a task of the transferring competent authority, which is also responsible for determining that no fundamental rights or freedoms of the individuals override the public interest justifying the transfer. Such transfers need to be documented and the transferring competent authority has to inform the competent supervisory authority.[778]

Finally, and in relation to third countries and international organisations, the directive also requires the development of international cooperation mechanisms to facilitate the effective enforcement of the legislation, and so helps data protection supervisory authorities to cooperate with their foreign counterparts.[779]

Independent supervision and remedies for data subjects

Each Member State must ensure that one or more independent national supervisory authorities are responsible for advising and monitoring the application of the provisions adopted pursuant to the directive.[780] The supervisory authority established for the purpose of the directive may be the same as the supervisory authority established under the General Data Protection Regulation, but Member States are free to designate a different authority, provided it meets the criteria of independence. Supervisory authorities shall also hear claims lodged by any person concerning the protection of his or her rights and freedoms regarding the processing of personal data by competent authorities.

Where the exercise of the data subject's rights is refused on compelling grounds, the data subject must have a right to appeal to the competent national supervisory authority and/or to a court. If a person suffers damage due to a violation of the national law implementing the directive, he or she is entitled to compensation

777 *Ibid.*, Art. 38 (1).

778 *Ibid.*, Art. 37 (3).

779 *Ibid.*, Art. 40.

780 *Ibid.*, Art. 41.

from the controller or any other authority competent under Member State law.[781] Generally, data subjects must have access to a judicial remedy for any breach of their rights guaranteed by national law implementing the directive.[782]

8.3. Other specific legal instruments on data protection in law enforcement matters

In addition to the Data Protection Directive for Police and Criminal Justice Authorities, the exchange of information held by Member States in specific areas is regulated by a number of legal instruments – such as Council Framework Decision 2009/315/JHA on the organisation and content of the exchange of information extracted from the criminal record between Member States, Council Decision 2000/642/JHA concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information, and Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.[783]

Importantly, cross-border cooperation[784] between the competent authorities increasingly involves the exchange of immigration data. This area of law is not considered a part of police and criminal justice matters but is in many respects relevant to the work of police and justice authorities. The same is true of data on goods being imported into or exported from the EU. The elimination of internal border controls within the Schengen area has heightened the risk of fraud, making it necessary for Member States to intensify cooperation, notably by enhancing cross-border information exchange, to more effectively detect and prosecute violations of national and EU customs law. Additionally, in recent years the world has seen an increase

781 *Ibid.*, Art. 56.

782 *Ibid.*, Art. 54.

783 Council of the European Union (2009), Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ 2009 L 93; Council of the European Union (2000), Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information, OJ 2000 L 271; Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386.

784 European Commission (2012), *Communication from the Commission to the European Parliament and the Council – Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)*, COM(2012) 735 final, Brussels, 7 December 2012.

in serious and organised crime and terrorism, which can involve international travel and has revealed a need for increased police and law-enforcement cross-border cooperation in many cases.[785]

The Prüm Decision

An important example of institutionalised cross-border cooperation by exchange of nationally held data is Council Decision 2008/615/JHA, along with its implementing provisions in Decision 2008/615/JHA, on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (Prüm Decision), which incorporated the Prüm Treaty into EU law in 2008.[786] The Prüm Treaty was an international police cooperation agreement signed in 2005 by Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Spain.[787]

The Prüm Decision aims to help signatory Member States improve information sharing for the purpose of preventing and combating crime in three fields: terrorism, cross-border crime and illegal migration. For this purpose, the decision sets out provisions with regard to:

- automated access to DNA profiles, fingerprint data and certain national vehicle registration data;
- the supply of data in relation to major events that have a cross-border dimension;
- the supply of information to prevent terrorist offences;
- other measures for stepping up cross-border police cooperation.

785 See European Commission (2011), Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, Brussels, 2 February 2011, p. 1.

786 Council of the European Union (2008), Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ 2008 L 210.

787 Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration.

The databases that are made available under the Prüm Decision are governed entirely by national law, but the exchange of data is additionally governed by the decision, whose compatibility with the Data Protection Directive for Police and Criminal Justice Authorities will have to be assessed. The competent bodies for supervision of such data flows are the national data protection supervisory authorities.

Framework Decision 2006/960/JHA – the Swedish Initiative

Framework Decision 2006/960/JHA (Swedish Initiative)[788] represents another example of cross-border cooperation with regard to the exchange of data held at national level by law enforcement authorities. The Swedish Initiative specifically focuses on the exchange of intelligence and information and provides for specific data protection rules in Article 8.

According to this instrument, the use of the information and intelligence exchanged must be subject to the national data protection provisions of the Member State receiving the information, according to the same rules as if they had been gathered in that Member State. Article 8 goes further by stating that when providing information and intelligence, the competent law enforcement authority may impose conditions that are in accordance with its national law on their use by the receiving competent law enforcement authority. Those conditions may also apply to the reporting of the result of the criminal investigation or to criminal intelligence operations for which the exchange of information and intelligence had been required. However, when national law provides for exceptions to the restrictions on use (e.g. for judicial authorities, legislative bodies, etc.), the information and intelligence may only be used after prior consultation with the communicating Member State.

Information and intelligence provided may be used:

- for the purposes for which it has been supplied; or
- to prevent an immediate and serious threat to public security.

Processing for other purposes can be permitted, but only upon prior authorisation of the communicating Member State.

788 Council of the European Union (2006), Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386/89 of 29 December 2006.

The Swedish Initiative further states that the personal data processed must be protected in accordance with international instruments such as the:

- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;[789]
- Additional Protocol of 8 November 2001 to that Convention, regarding Supervisory Authorities and Transborder Data Flows;[790]
- Recommendation No. R(87) 15 of the Council of Europe Regulating the Use of Personal Data in the Police Sector.[791]

The EU PNR Directive

Passenger Name Record (PNR) data relate to the information on air passengers collected by and held in the carriers' reservation and departure control systems for their own commercial purposes. These data contain several different types of information, such as travel dates, travel itinerary, ticket information, contact details, the travel agent where the flight was booked, means of payment used, seat number and baggage information.[792] Processing PNR data may help law enforcement authorities identify known or potential suspects and carry out assessments based on travel patterns and other indicators typically associated with criminal activities. An analysis of PNR data also allows retrospective tracking of the travel routes and contacts of persons suspected to have been involved in criminal activities, which can enable law enforcement authorities to identify criminal networks.[793] The EU has concluded some agreements with third countries for the exchange of PNR data, as explained in Section 7. In addition, it has introduced PNR data processing within the EU, through Directive 2016/681/EU on the use of PNR data for the prevention,

789 Council of Europe (1891), Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS n. 108.

790 Council of Europe (2001), Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, ETS n. 108.

791 Council of Europe (1987), Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies).

792 European Commission (2011), Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, Brussels, 2 February 2011, p. 1.

793 European Commission (2015), Fact Sheet Fighting terrorism at EU level, an overview of Commission's actions, measures and initiatives, Brussels, 11 January 2015.

detection, investigation and prosecution of terrorist offences and serious crime (EU PNR Directive).[794] This directive provides for obligations for air carriers to transmit PNR data to the competent authorities and establishes strict data protection safeguards for the processing and collection of such data. The EU PNR Directive applies to international flights to and from the EU, but also to intra-EU flights if a Member State so decides.[795]

The PNR data collected must only contain the information allowed by the EU PNR Directive. It must be retained in a single information unit, within a secure location in each Member State. PNR data must be depersonalised six months after its transmission from the air-carrier and retained for a maximum period of five years.[796] PNR data are exchanged between Member States; between Member States and Europol; and with third countries, but only on a case-by-case basis.

The transmission and processing of the PNR data and the rights safeguarded for data subjects must be in line with the Data Protection Directive for Police and Criminal Justice Authorities and must ensure the high level of protection of privacy and personal data required by the Charter, Modernised Convention 108 and the ECHR.

The independent national supervisory authorities competent under the Data Protection Directive for Police and Criminal Justice Authorities are also responsible for advising on and monitoring the application of the provisions adopted by the Member States, pursuant to the EU PNR Directive.

Retention of telecommunications data

The Data Retention Directive[797] – declared invalid on 8 April 2014 in *Digital Rights Ireland* – obliged communication service providers to keep metadata available for the specific purpose of fighting serious crime, for at least six but no more than 24 months, regardless of whether or not the provider still needed these data for billing purposes or to technically provide the service.

794 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ 2016 L 119, p. 132.

795 PNR Directive, L 119, p. 132, Art. 1 (1) and Art. 2 (1).

796 *Ibid.*, Art. 12 (1) and Art. 12 (2).

797 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications' services or of public communications' networks and amending Directive 2002/58/EC, OJ 2006 L 105.

The retention of telecommunications data clearly interferes with the right to data protection.[798] Whether or not this interference is justified has been contested in several court procedures in EU Member States.[799]

Example: In *Digital Rights Ireland* and *Kärntner Landesregierung and Others*,[800] the Digital Rights group and Mr Seitlinger brought an action before the High Court in Ireland and the Constitutional Court in Austria, respectively, challenging the legality of national measures allowing the retention of electronic telecommunications data. Digital Rights asked the Irish court to declare invalid Directive 2006/24 and the part of national criminal law relating to terrorist offences. Similarly, Mr Seitlinger and more than 11,000 other applicants challenged and requested the annulment of a provision of the Austrian legislation on telecommunications that transposed Directive 2006/24.

In addressing these requests for preliminary rulings, the CJEU declared the Data Retention Directive to be invalid. According to the CJEU, the data that could be retained under the directive provided precise information about individuals when taken as a whole. Furthermore, the CJEU examined the seriousness of the interference with the fundamental rights to respect for private life and to the protection of personal data. It found that the retention satisfies an objective of public interest – namely the fight against serious crime and, thus, public security. Nevertheless, the CJEU stated that the EU legislator had violated the principle of proportionality by adopting the directive. Even though the directive may be appropriate to obtaining the required goal, "the wide-ranging and particularly serious interference of the Directive with the fundamental rights to respect privacy and the protection of personal data is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary."

798 EDPS (2011), *Opinion of 31 May 2011 on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)*, 31 May 2011.

799 Germany, Federal Constitutional Court *(Bundesverfassungsgericht)*, 1 BvR 256/08, 2 March 2010; Romania, Federal Constitutional Court (*Curtea Constituþionalã a României*), No. 1258, 8 October 2009; the Czech Republic, Constitutional Court (*Ústavní soud České republiky*), 94/2011 Coll., 22 March 2011.

800 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [GC], 8 April 2014, para. 65.

Data retention is allowed, in the absence of specific legislation on data retention, as an exception to the confidentiality of telecommunications data under Directive 2002/58/EC (Directive on privacy and electronic communications),[801] as a preventive measure, but must be solely for the purpose of fighting serious crime. Such retention must be limited to what is strictly necessary with regard to the categories of data retained, the means of communication affected, the persons concerned and the chosen duration of the retention. National authorities may have access to the retained data under strict conditions, including prior review by an independent authority. The data must be retained within the EU.

Example: Following the *Digital Rights Ireland* and *Kärntner Landesregierung and Others*[802] judgment, two more cases were brought before the CJEU in relation to the general obligation imposed in Sweden and in the UK for providers of electronic communication services to retain telecommunications data, as required by the invalidated Data Retention Directive. In *Tele2 Sverige* and *Home Department v. Tom Watson and Others*,[803] the CJEU ruled that national legislation that prescribes the general and indiscriminate retention of data without requiring any relationship between the data which must be retained and a threat to public security, and without specifying any conditions – e.g. time period for the retention, geographical area, group of persons likely to be involved in a serious crime – exceeds the limits of what is strictly necessary and cannot be considered justified within a democratic society, as required by Directive 2002/58/EC, read in the light of the EU Charter of Fundamental Rights.

Outlook

In January 2017, the European Commission published a proposal for a Regulation concerning the respect for private life and the protection of personal data in

801 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications' sector (Directive on privacy and electronic communications), OJ 2002 L 201.

802 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [GC], 8 April 2014.

803 CJEU, Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others* [GC], 21 December 2016.

electronic communications, meant to repeal and replace Directive 2002/58/EC.[804] The proposal does not include any specific provisions on data retention. However, it provides that Member States may restrict certain obligations and rights under the regulation by law, when such a restriction constitutes a necessary and proportionate measure for safeguarding specific public interests, including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.[805] Therefore, Member States would be able to keep or create national data retention frameworks that provide for targeted retention measures, in so far as such frameworks comply with Union law, taking into account the case law of the CJEU on the interpretation of the e-Privacy Directive and the EU Charter of Fundamental Rights.[806] At the time of drafting of the handbook, discussions on the adoption of the regulation were ongoing.

EU-US Umbrella Agreement on the protection of personal data exchanged for law enforcement purposes

On 1 February 2017, the EU-US Umbrella agreement for the processing of personal data for the prevention, investigation, detection, and prosecution of criminal offences with the US came into force.[807] The EU-US Umbrella agreement aims to ensure a high level of data protection for EU citizens while enhancing the cooperation of EU and US law enforcement authorities. It complements existing EU-US and Member State-US agreements between law enforcement authorities while also helping to put in place clear and harmonised data protection rules for future agreements in this field. In that regard, the agreement aims to establish a lasting legal framework to facilitate the exchange of information.

The agreement does not in itself provide a suitable legal basis for the exchange of personal data, but instead offers suitable data protection safeguards to the

804 European Commission (2017), *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, COM(2017) 10 final, Brussels, 10 January 2017.

805 *Ibid.*, Recital 26.

806 See the explanatory memorandum to the Proposal for a Regulation on Privacy and Electronic Communications COM(2017) 10 final, point 1.3.

807 See Council of the EU (2016), "*Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign 'Umbrella agreement'*", Press Release 305/16, 2 June 2016.

individuals concerned. It covers all processing of personal data necessary for the prevention, investigation, detection, and prosecution of criminal offences, including terrorism.[808]

The agreement sets out multiple safeguards to ensure that personal data are only used for the purposes specified in the agreement. In particular, it provides the following protection to EU citizens:

- limitations on the use of data: personal data may only be used for the purpose of preventing, investigating, detecting or prosecuting criminal offences;
- protection against arbitrary and unjustifiable discrimination;
- onward transfers: any onward transfer to a non-US, non-EU country or international organisation must be subject to the prior consent of the competent authority of the country which originally transferred the data;
- data quality: personal data need to be kept considering their accuracy, relevance, timeliness and completeness;
- security of the processing, including notification of personal data breaches;
- processing of sensitive data is only allowed under appropriate safeguards in accordance with law;
- retention periods: personal data may not be retained for longer than necessary or appropriate;
- access and rectification rights: any individual is entitled to access their personal data, subject to certain conditions, and will be able to request the data is corrected if it is inaccurate;

808 Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses of 18 May 2016, (OR.en) 8557/16, Art. 3(1). See also Commission notification on the EU-US data protection agreement negotiations of 26 May 2010, MEMO/10/216 and the EU Commission Press Release (2010) on high privacy standards in EU-US data protection agreement of 26 May 2010, IP/10/609.

- automated decisions require appropriate safeguards, including the possibility to obtain human intervention;

- effective oversight, including cooperation between EU and US oversight authorities; and

- judicial redress and enforceability: EU citizens have the right[809] to seek judicial redress before US courts in cases where the US authorities deny access or rectification, or unlawfully disclose their personal data.

Under the 'Umbrella agreement', a system has also been set up to notify the competent supervisory authority in the Member State of affected individuals about any data protection breaches, where necessary. The legal safeguards provided by the agreement ensure the equal treatment of EU citizens in the US where there is a privacy breach.[810]

8.3.1. Data protection in EU judicial and law enforcement agencies

Europol

Europol, the EU's law enforcement agency, is headquartered in The Hague, with Europol National Units (ENUs) in each Member State. Europol was established in 1998; its present legal status as an EU institution is based on the Regulation on the European Union Agency for Law Enforcement Cooperation (Europol Regulation).[811] The object of Europol is to assist with the prevention and investigation of organised crime, terrorism and other forms of serious crime, as listed in Annex I of the Europol Regulation, which affect two or more Member States. It does so by exchanging

809 The US Judicial Redress Act was signed into law by President Obama on 24 February 2016.

810 The European Data Protection Supervisor issued an Opinion on the EU-US Agreement recommending, among others, the following adaptations: 1) adding 'for the specific purposes for which they were transferred' to the article dealing with retention of data not longer than necessary and appropriate and 2) excluding bulk transfer of sensitive data, which may be possible. See European Data Protection Supervisor, Opinion 1/2016, *Preliminary Opinion on the agreement between the United State of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences*, § 35.

811 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ 2016 L 135, p. 53.

information and by acting as the EU's information hub, providing intelligence analyses and threat assessments.

To achieve its aims, Europol has established the Europol Information System, which provides a database for Member States to exchange criminal intelligence and information through their ENUs. The Europol Information System may be used to make available data which relate to: persons who are suspects or who have been convicted of a criminal offence which is subject to Europol's competence; or persons regarding whom there are factual indications that they will commit such offences. Europol and ENUs may enter data directly into the Europol Information System and retrieve data therefrom. Only the party which entered the data into the system may modify, correct or delete them. EU bodies, third countries and international organisations may also provide information to Europol.

Information, including personal data, can also be obtained by Europol from publicly available sources such as the internet. Transfers of personal data to EU bodies are allowed only if necessary for the performance of the task of Europol or the recipient EU body. Transfers of personal data to third countries or international organisations are allowed only if the European Commission decides that the country or international organisation in question ensures an adequate level of data protection ('adequacy decision'), or if there is an international or cooperation agreement. Europol can receive and process personal data from private parties and private persons under the strict conditions that those data are transferred by an ENU in accordance with its national law, by a contact point in a third country or an international organisation with which there is established cooperation through a cooperation agreement, or by an authority of a third country or an international organisation which is subject to an adequacy decision or with which the EU has concluded an international agreement. All information exchanges are done through a Secure Information Exchange Network Application (SIENA).

In response to new developments, specialised centres have been established within Europol. The European Cybercrime Centre was established within Europol in 2013.[812] The centre serves as the EU information hub on cybercrime, contributing to faster reactions in the event of online crimes, developing and deploying digital forensic capabilities and delivering best practice on cybercrime investigations. The centre focuses on cybercrime that:

812 See also EDPS (2012), *Opinion of the Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre*, Brussels, 29 June 2012.

- is committed by organised groups to generate large criminal profits, such as online fraud;
- causes serious harm to the victim, such as online child sexual exploitation;
- affects critical infrastructure or information systems within the EU.

The European Counter Terrorism Centre (ECTC) was created in January 2016 to provide operational support to Member States in investigations related to terrorist offences. It cross-checks live operational data against the data Europol already has, quickly bringing financial leads to light, and analyses all available investigative details to assist in compiling a structured picture of a terrorist network.[813]

The European Migrant Smuggling Centre (EMSC) was established in February 2016, following a Council meeting in November 2015, to support Member States in targeting and dismantling criminal networks involved in migrant smuggling. It acts as an information hub supporting the EU Regional Task Force offices in Catania (Italy) and Piraeus (Greece), which assist national authorities in several areas, including intelligence sharing, criminal investigations and the prosecution of criminal people-smuggling networks.[814]

The data protection regime governing Europol's activities is enhanced and draws on the principles of the EU Institutions Data Protection Regulation[815] and is also consistent with the Data Protection Directive for Police and Criminal Justice Authorities, Modernised Convention 108 and the Police Recommendation.

The processing of personal data in respect of victims of a criminal offence, witnesses or other persons who can provide information concerning criminal offences, or in respect of persons under the age of 18, is allowed if it is strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives.[816] The processing of sensitive personal data is prohibited, unless it is strictly necessary and proportionate for preventing or combating crime that falls within

813 See Europol's webpage on the ECTC.

814 See Europol's webpage on the EMSC.

815 Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, OJ 2001 L 8.

816 Europol Regulation, Art. 30 (1).

Europol's objectives and if those data supplement other personal data processed by Europol.[817] In both these cases only Europol can access the relevant data.[818]

The storage of data is allowed only for a necessary and proportionate period of time and its continuation is subject to a review every three years, without which the data are erased automatically.[819]

Europol is allowed, under certain conditions, to transfer personal data to an EU body or to an authority of a third country or to an international organisation directly.[820] Data breaches, if likely to severely and adversely affect the rights and freedoms of the data subjects concerned, need to be communicated to them without undue delay.[821] At the Member State level, a national supervisory authority will be appointed to monitor Europol processing of personal data.[822]

The EDPS is responsible for monitoring and ensuring the protection of fundamental rights and freedoms of natural persons with regard to the processing of personal data by Europol, and for advising Europol and data subjects on all matters concerning the processing of personal data. To that end, the EDPS acts as an investigating and complaints body and acts in close cooperation with the national supervisory authorities.[823] EDPS and the national supervisory authorities will meet at least twice a year in the Cooperation Board, which has an advisory function.[824] Member States are obliged to establish a supervisory authority by law, competent to monitor the permissibility of the transfer of personal data from state level to Europol and the retrieval and any communication with Europol of personal data by the Member State.[825] Member States are also required to ensure that the national supervisory authority can act completely independently when performing their tasks and duties under the Europol Regulation.[826] To verify the lawfulness of data processing, self-monitor its activities and ensure data integrity and security, Europol keeps logs or

817 *Ibid.*, Art. 30 (2).
818 *Ibid.*, Art. 30 (3).
819 *Ibid.*, Art. 31.
820 *Ibid.*, Art. 24 and Art. 25, respectively.
821 *Ibid.*, Art. 35.
822 Europol Regulation, Art. 42.
823 *Ibid.*, Art. 43 and Art. 44.
824 *Ibid.*, Art. 45.
825 *Ibid.*, Art. 42 (1).
826 *Ibid.*, Art. 42 (1).

documentation of its data processing activities. These logs contain information on processing operations in automated processing systems related to collection, alteration, consultation, disclosure, combination and erasure.[827]

An appeal against a decision of the EDPS can be brought before the CJEU.[828] Any individual who has suffered damage as a result of an unlawful data processing operation has the right to receive compensation for damage suffered, either from Europol or from the responsible Member State, by bringing an action before the CJEU in the first case, or before the competent national court in the second case.[829] In addition, a specialised Joint Parliamentary Scrutiny Group (JPSG) of the national parliaments and the European Parliament can scrutinise Europol's activities.[830] Every individual has a right of access to any personal data that Europol may be holding about him or her, in addition to a right to request that these personal data be checked, corrected or erased. These may be subject to exemptions and limitations.

Eurojust

Eurojust, set up in 2002, is an EU body headquartered in The Hague. It promotes judicial cooperation in investigations and prosecutions relating to serious crime concerning at least two Member States.[831] Eurojust is competent to:

- stimulate and improve coordination of investigations and prosecutions between the competent authorities of the various Member States;
- facilitate the execution of requests and decisions relating to judicial cooperation.

The functions of Eurojust are performed by national members. Each Member State delegates one judge or prosecutor to Eurojust, whose status is subject to the national law and is empowered with the necessary competences to perform the

827 *Ibid.*, Art. 40.

828 *Ibid.*, Art. 48.

829 *Ibid.*, Art. 50.

830 *Ibid.*, Art. 51.

831 Council of the European Union (2002), Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ 2002 L 63; Council of the European Union (2003), Council Decision 2003/659/JHA of 18 June 2003 amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ 2003 L 44; Council of the European Union (2009), Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ 2009 L 138 (Eurojust Decisions).

tasks necessary to stimulate and improve judicial cooperation. Additionally, the national members act jointly as a college to carry out special Eurojust tasks.

Eurojust may process personal data as far as this is necessary to achieve its objectives. This is limited, however, to specific information regarding persons who are suspected of having committed or having taken part in, or have been convicted of, a criminal offence subject to Eurojust's competence. Eurojust may also process certain information regarding witnesses or victims of criminal offences subject to Eurojust's competence.[832] In exceptional circumstances, Eurojust may, for a limited period of time, process more extensive personal data relating to the circumstances of an offence where such data are immediately relevant to an ongoing investigation. Within its remit of competence, Eurojust may cooperate with other EU institutions, bodies and agencies and exchange personal data with them. Eurojust may also cooperate and exchange personal data with third countries and organisations.

In relation to data protection, Eurojust must guarantee a level of protection at least equivalent to the principles of Modernised Convention 108 and its subsequent amendments. In cases of data exchange, specific rules and limitations must be observed, which are put in place either in cooperation agreement or working arrangement in accordance with Eurojust Council Decisions and Eurojust Data Protection Rules.[833]

An independent Joint Supervisory Body (JSB) has been established at Eurojust with the task of monitoring the processing of personal data performed by Eurojust. Individuals may appeal to the JSB if they are not satisfied with Eurojust's decision to a request for access, correction, blocking or erasure of personal data. Where Eurojust processes personal data unlawfully, Eurojust shall be liable in accordance with the national law of the Member State where its headquarters is located, the Netherlands, for any damage caused to the data subject.

Outlook

The European Commission presented a proposal on a regulation to reform Eurojust in July 2013. This proposal was accompanied by a proposal to establish a European Public Prosecutor's Office (see below). This regulation aims to streamline the

832 Consolidated version of the Council Decision 2002/187/JHA as amended by Council Decision 2003/659/JHA and by Council Decision 2009/426/JHA, Art. 15 (2).

833 Rules of Procedure on the Processing and Protection of Personal Data at Eurojust, OJ 2005 C 68/01, 19 March 2005, p. 1.

functions and structure to be line with the Lisbon Treaty. Furthermore, the reform's goal is to establish a clear division between the operational tasks of Eurojust, performed by the Eurojust College, and its administrative tasks. This will also enable Member States to focus more on the operational tasks. A new Executive Board will be established to assist the college when performing administrative tasks.[834]

European Public Prosecutor's Office

Member States have exclusive competence in prosecuting the criminal offences of fraud and improper application of the EU budget, which also have potential cross-border implications. The significance of investigating, prosecuting and bringing to justice the perpetrators of such offences has increased, especially given the ongoing economic crisis.[835] The European Commission has proposed a Regulation on the establishment of an independent European Prosecutor's Office (EPPO)[836] with the objective of combating criminal offences affecting EU financial interests. The EPPO will be established through the enhanced cooperation procedure, which allows a minimum of nine Member States to establish advanced cooperation in an area within EU structures, without the other EU countries being involved.[837] Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Estonia, Finland, France, Germany, Greece, Latvia, Lithuania, Luxembourg, Portugal, Romania, Slovenia, Slovakia and Spain have all joined the enhanced cooperation; Austria and Italy have expressed their intention to join.[838]

The EPPO will be competent to investigate and prosecute EU fraud and other crimes affecting EU financial interests, with an aim of efficiently coordinating investigations and prosecutions across the different national legal orders and of improving the use of resources and the exchange of information at European level.[839]

834 See the European Commission's webpage on Eurojust.

835 See European Commission (2013), Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office, COM(2013) 534 final, Brussels, 17 July 2013, p. 1 and the Commission's webpage on the EPPO.

836 European Commission (2013), Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office, COM(2013) 534 final, Brussels, 17 July 2013.

837 Treaty on the Functioning of the EU, Art. 86 (1) and Art. 329 (1).

838 See Council of the European Union (2017), "*20 member states agree on the details of creating the European Public Prosecutor's Office (EPPO)*", press release, 8 June 2017.

839 European Commission (2013), Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office, COM(2013) 534 final, Brussels, 17 July 2013, p. 1 and pp. 51–51. See also the Commission's webpage on the EPPO.

The EPPO will be headed by a European Public Prosecutor, with at least one delegated European Prosecutor located in each Member State in charge of carrying out the investigations and prosecutions in that Member State.

The proposal sets out strong safeguards to guarantee the rights of the persons involved in the EPPO's investigations as laid down in national law, EU law and the EU Charter of Fundamental Rights. Investigatory measures that touch mostly on fundamental rights will need prior authorisation by a national court.[840] The EPPO's investigations will be subject to judicial review by the national courts.[841]

The EU Institutions Data Protection Regulation[842] will apply to the processing of administrative personal data performed by the EPPO. For the processing of personal data related to operational matters, like Europol, the EPPO will have a standalone data protection regime similar to the one governing the activities of Europol and Eurojust, given that the exercise of the EPPO's functions will involve the processing of personal data with law enforcement and prosecution authorities at Member State level. The EPPO data protection rules are therefore almost identical to the rules of the Data Protection Directive for Police and Criminal Justice Authorities. According to the Proposal for the establishment of the EPPO, the processing of personal data must comply with the principles of lawfulness and fairness, purpose limitation, data minimisation, accuracy, integrity and confidentiality. The EPPO must make, as far as possible, a clear distinction between the personal data of different types of data subjects, such as persons convicted of a criminal offence, persons who are merely suspects, victims and witnesses. It must also seek to verify the quality of the personal data processed and to distinguish, as far as possible, personal data based on facts from personal data based on personal assessments.

The proposal contains provisions on the rights of data subjects, notably the rights to information, to access their personal data, to rectification, erasure and restriction of processing, and provides that such rights may also be exercised indirectly, through the EDPS. It also embodies the principles of security of processing and accountability, requiring that the EPPO implements appropriate technical and organisational measures to ensure a level of security appropriate to the risks posed by the processing,

840 European Commission (2013), Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office, COM(2013) 534 final, Brussels, 17 July 2013, Art. 26 (4).

841 *Ibid.*, Art. 36.

842 Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, OJ 2001 L 8.

to keep records of all processing activities and to carry out a data protection impact assessment prior to the processing, where a type of processing (for example, processing involving the use of new technologies) is likely to result in high risk to the rights of individuals. Finally, the proposal provides for the designation of a Data Protection Officer by the college, who must be properly involved in all matters relating to the protection of personal data and must ensure the EPPO's compliance with the applicable data protection legislation.

8.3.2. Data protection in EU-level joint information systems

In addition to data exchange between Member States and the creation of specialised EU authorities for fighting transborder crime, such as Europol, Eurojust and the EPPO, several joint information systems have been established at the EU level to enable and facilitate cooperation and data exchange between the competent national and EU authorities for specified purposes in the areas of border protection, immigration and asylum and customs. As the Schengen area was first created through an international agreement operating independently from EU law, the Schengen Information System (SIS) developed out of multilateral agreements and was subsequently brought under EU law. The Visa Information System (VIS), Eurodac, Eurosur and the Customs Information System (CIS) were created as instruments governed by EU law.

The supervision of these systems is shared between the national supervisory authorities and the EDPS. To ensure a high level of protection, these authorities collaborate within Supervision Coordination Groups (SCGs), which refers to the following large-scale IT systems: 1) Eurodac; 2) Visa Information System; 3) Schengen Information System; 4) Customs Information System and 5) Internal Market Information System.[843] The SCGs usually meet twice a year, under the authority of an elected Chair, and adopt Guidelines, discuss cross-border cases or adopt common frameworks for inspections.

The European Agency for Large-scale Information Technology Systems (eu-LISA),[844] established in 2012, is responsible for the operational management of the second-generation Schengen Information System (SIS II), the Visa Information System (VIS)

843 See the European Data Protection Supervisor's webpage on Supervision Coordination.

844 Regulation (EU) No. 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ 2011 L 286.

and Eurodac. The core task of the eu-LISA is to ensure the effective, secure and continuous operation of the information technology systems. It is also responsible for the adoption of necessary measures to ensure the security of the systems and the security of data.

The Schengen Information System

In 1985, several Member States of the former European Community entered into the Agreement between the states of the Benelux Economic Union, Germany and France on the gradual abolition of checks at their common borders (Schengen Agreement), aiming to create an area for the free movement of persons, unhindered by border controls within the Schengen territory.[845] To counterbalance the threat to public security that could arise from open borders, strengthened border controls at the Schengen area's external borders were established, as well as close cooperation between national police and justice authorities.

As a consequence of the accession of additional states to the Schengen Agreement, the Schengen system was finally integrated into the EU legal framework by the Treaty of Amsterdam.[846] Implementation of this decision took place in 1999. The newest version of the Schengen Information System, the so-called SIS II, came into operation on 9 April 2013. It now serves most EU Member States,[847] plus Iceland, Liechtenstein, Norway and Switzerland.[848] Europol and Eurojust also have access to SIS II.

SIS II consists of a central system (C-SIS), a national system (N-SIS) in each Member State, and a communication infrastructure between the central system and the national systems. C-SIS contains certain data entered by the Member States on persons and objects. SIS is used by national border control, police, customs, visa

845 Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ 2000 L 239.

846 European Communities (1997), Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, OJ 1997 C 340.

847 Croatia, Cyprus and Ireland are carrying out preparatory activities to integrate into the SIS II, but are not yet part thereof. See the information on the Schengen Information System available on the website of the European Commission Directorate General for Migration and Home Affairs.

848 Regulation (EC) No. 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System, OJ 2006 L 381 (SIS II) and Council of the European Union (2007), Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System, (SIS II), OJ 2007 L 205.

and judicial authorities throughout the Schengen Area. Each of the Member States operates a national copy of the C-SIS, known as National Schengen Information Systems (N-SIS), which are constantly updated, thereby updating the C-SIS. There are different types of alerts in SIS:

- the person does not have the right to enter or stay in the Schengen territory; or
- the person or object is sought by judicial or law enforcement authorities (e.g. European Arrest Warrants, requests for discreet checks); or
- the person has been reported as missing; or
- goods, such as banknotes, cars, vans, firearms and identity documents, have been reported as stolen or lost property.

Where there is an alert, follow-up activities are to be initiated via the SIRENE bureaux. SIS II has new functionalities, such as the possibility of entering: biometric data, such as fingerprints and photographs; or new categories of alerts, such as stolen boats, aircrafts, containers or means of payment; enhanced alerts on persons and objects; and copies of European Arrest Warrants (EAWs) on persons wanted for arrest, surrender or extradition.

The SIS II is based on two acts that complement each other: the SIS II Decision[849] and the SIS II Regulation.[850] The EU legislator used different legal basis for the adoption of the decision and the regulation. The decision governs the use of SIS II for purposes covered by police and judicial cooperation in criminal matters (the former third pillar of the EU). The regulation applies to alert procedures falling under visas, asylum, immigration and other policies related to the free movement of persons (formerly the first pillar). The alert procedures for each pillar had to be regulated by separate acts, given that the two legal acts were adopted before the Treaty of Lisbon and the abolition of the pillars structure.

849 Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205, 7 August 2007.

850 Regulation (EC) No. 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 28 December 2006.

Both legal acts contain rules on data protection. The SIS II Decision prohibits the processing of sensitive data.[851] The processing of personal data shall be covered by the scope of Modernised Convention 108.[852] Furthermore, persons have the right to have access to the personal data related to them, which is entered in SIS II.[853]

The SIS II Regulation regulates the conditions and procedures for entering and processing alerts regarding refusals for entry or stay of non-EU citizens. It also provides rules for exchanging supplementary and additional information for the purposes of entry or stay in a Member State.[854] This regulation also contains rules on data protection. Sensitive categories of data, as referred to in Article 9(1) of the General Data Protection Regulation, are not allowed to be processed.[855] The SIS II Regulation also contains certain rights for the data subject, which are:

- the right to access to personal data related to the data subject;[856]
- the right to correct factually inaccurate data;[857]
- the right to delete unlawfully stored data;[858] and
- the right to be informed if there is an alert issued against the data subject. The information shall be in writing and be accompanied with a copy or a reference to the national decision to issue the alert.[859]

The right to be informed shall not be provided, if 1) the personal data have not been obtained from the data subject and providing that information is impossible or requires a disproportionate effort, 2) the data subject already possesses the information or 3) if national law allows for a restriction based on, amongst other things, safeguarding national security or preventing criminal offences.[860]

851 SIS II Decision, Art. 56; SIS II Regulation, Art. 40.
852 SIS II Decision, Art. 57.
853 SIS II Decision, Art. 58; SIS II Regulation, Art. 41.
854 SIS II Regulation, Art. 2.
855 *Ibid.*, Art. 40.
856 *Ibid.*, Art. 41 (1).
857 *Ibid.*, Art. 41 (5).
858 *Ibid.*, Art. 41 (5).
859 *Ibid.*, Art. 42 (1).
860 *Ibid.*, Art. 42 (2).

For both the SIS II Decision and SIS II Regulation, access rights of individuals concerning the SIS II may be exercised in any Member State, and will be dealt with in accordance with the national law of that Member State.[861]

> Example: In *Dalea v. France*,[862] the applicant was denied a visa to visit France, as the French authorities had reported to the Schengen Information System that he should be refused entry. The applicant unsuccessfully sought access and rectification or deletion of the data before the French Data Protection Commission and, ultimately, before the Council of State. The ECtHR held that the reporting of the applicant to the Schengen Information System had been in accordance with the law and had pursued the legitimate aim of protecting national security. Since the applicant did not show how he had actually suffered as a result of the denial of entry into the Schengen area, and since sufficient measures to protect him from arbitrary decisions were in place, the interference with his right to respect for private life had been proportionate. The applicant's complaint under Article 8 was thus declared inadmissible.

The competent national supervisory authority in each Member State supervises the domestic N-SIS. The national supervisory authority must ensure that an audit of the data-processing operations within the domestic N-SIS takes place at least every four years.[863] The national supervisory authorities and the EDPS cooperate and ensure coordinated supervision of the N-SIS, while the EDPS is responsible for the supervision of the C-SIS. For the sake of transparency, a joint report of activities shall be sent to the European Parliament, the Council and eu-LISA every two years. The SIS II's Supervision Coordination Group (SCG) has been set up to ensure the SIS's supervision coordination and it meets up to twice a year. This group consists of the EDPS and representatives of the supervisory authorities of those Member States that have implemented SIS II, as well as Iceland, Liechtenstein, Norway and Switzerland, since the SIS applies to them as well, given that they are members of Schengen.[864] Cyprus, Croatia and Ireland are not yet part of SIS II and therefore only participate as observers to the SCG. Within the context of the SCG, the EDPS and the national supervisory authorities cooperate actively, by exchanging information, assisting each other in the conducting of audits and inspections, designing harmonised proposals

861 SIS II Regulation, Art. 41 (1) and SIS II Decision, Art. 58.

862 ECtHR, *Dalea v. France,* No. 964/07, 2 February 2010.

863 SIS II Regulation, Art. 60 (2).

864 See the European Data Protection Supervisor's webpage on the Schengen Information System.

for common solutions to potential problems and in promoting awareness of data protection rights.[865] The SIS II SCG also adopts guidelines to assist data subjects. One example is the guide to assist data subjects in exercising their access rights.[866]

Outlook

In 2016, the European Commission carried out an evaluation of the SIS[867] showing that national mechanisms have been put in place to enable data subjects to access, correct, and delete their personal data in SIS II or to obtain compensation in connection with inaccurate data. To improve the efficiency and effectiveness of SIS II, the European Commission brought forward three proposals for regulations:

- a regulation on the establishment, operation and use of the SIS in the field of border checks, which will repeal the SIS II Regulation;
- a regulation on the establishment, operation and use of the SIS in the field of police cooperation and judicial cooperation in criminal matters, which will repeal, among other things, the SIS II Decision; and
- a regulation on the use of the SIS for the return of illegally-staying third country nationals.

Importantly, the proposals allow the processing of other categories of biometric data – in addition to photographs and fingerprints, which are already part of the current SIS II regime. Facial fingerprints, palm prints and DNA profiles will also be stored in the SIS database. In addition, while the SIS II Regulation and SIS II decision provided for a possibility to search with fingerprints to identify a person, the proposals make this search mandatory if the identity of the person cannot be ascertained in any other way. Facial images, photographs and palm prints will be used to search the system and identify people, when this becomes technically possible. The new rules on biometric attributes pose particular risks for the rights of individuals. In its opinion

865 SIS II Regulation, Art. 46 and SIS II Decision, Art. 62.

866 See SIS II SCG, *The Schengen Information System. A guide for exercising the right of access*, available on the EDPS website.

867 European Commission (2016), Report from the Commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with Art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No. 1987/2006 and Art. 59 (3) and 66 (5) of Decision 2007/533/JHA, COM(2016) 880 final, Brussels, 21 December 2016.

on the Commission proposals,[868] the EDPS noted that biometric data are highly sensitive and their introduction into such a large-scale database should be based on an evidence-based assessment of the need to include them in the SIS. In other words, the necessity of processing the new attributes should be demonstrated. The EDPS also considered that there is a need to further clarify what type of information can be included in the DNA profile. Since the DNA profile can include sensitive information (the most notable example would be information-revealing health issues), the DNA profiles stored in the SIS should contain: "only the minimum information which is strictly necessary for the identification of the missing persons and exclude explicitly health information, racial origin and any other sensitive information."[869] The proposals, however, establish additional safeguards to limit the collection and further processing of data to that which is strictly necessary and operationally required, and access is restricted to persons who have an operational need to process the personal data.[870] The proposals also empower eu-LISA to produce data quality reports for Member States at regular intervals, in order to regularly review alerts to ensure data quality.[871]

The Visa Information System

The Visa Information System (VIS), also operated by the eu-LISA, was developed to support the implementation of a common EU visa policy.[872] The VIS allows Schengen states to exchange data concerning visa applicants through a fully centralised system which connects the consulates and embassies of the Schengen states situated in non-EU countries with the external border-crossing points of all Schengen states. The VIS processes data regarding applications for short-stay visas to visit or

868 EDPS (2017), EDPS Opinion on the new legal basis of the Schengen Information System, Opinion 7/2017, 2 May 2017.

869 *Ibid.*, para. 22.

870 European Commission (2016), Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No. 515/2014 and repealing Regulation (EC) No. 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU, COM(2016) 883 final, Brussels, 21 December 2016.

871 *Ibid.*, p. 15.

872 Council of the European Union (2004), Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), OJ 2004 L 213; Regulation (EC) No. 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, OJ 2008 L 218 (VIS Regulation); Council of the European Union (2008), Council Decision 2008/633/JHA of June 23 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ 2008 L 218.

to transit through the Schengen area. The VIS enables border authorities to verify, with the help of biometric attributes, notably fingerprints, whether or not the person presenting a visa is its rightful holder and to identify persons with no or fraudulent documents.

Regulation (EC) No. 767/2008 of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) regulates the conditions and procedures for transferring personal data regarding applications for short-stay visas. It also oversees the decisions taken on applications, including decisions to annul, revoke or extend the visa.[873] The VIS Regulation mainly covers data on the applicant, his or her visas, photographs, fingerprints, links to previous applications, and the application files of persons accompanying him or her, or data regarding inviting persons.[874] Access to the VIS in order to enter, amend or delete data is restricted exclusively to the visa authorities, whereas access to consulting data is provided to visa authorities and authorities competent for checks at the external border-crossing points, immigration checks and asylum.

Under certain conditions, competent national police authorities and Europol may request access to data entered into the VIS for the purpose of preventing, detecting or investigating terrorist and criminal offences.[875] Since the VIS has been designed as an instrument to support the implementation of the common visa policy, the principle of purpose limitation which, as explained in Chapter 3.2, requires that personal data is processed only for specified, explicit and legitimate persons, and must be adequate, relevant and not excessive in relation to the purposes for which the data are processed, would be violated if the VIS would turned into a law enforcement tool. For this reason, national law enforcement authorities and Europol are not granted routine access to the VIS database. Access may only be granted on a case-by-case basis and be accompanied by strict safeguards. The conditions and safeguards for access and consultation of the VIS by these authorities have been regulated in Council Decision 2008/633/JHA.[876]

873 VIS Regulation, Art. 1.

874 Art. 5 of the Regulation (EC) No. 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ 2008 L 218.

875 Council of the European Union (2008), Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ 2008 L 218.

876 *Ibid.*

Furthermore, the VIS Regulation provides for rights of data subjects. These are:

- The right to be informed by the responsible Member State of the identity and contact details of the data controller in charge of the processing of personal data within that Member State, the purposes for which their personal data will be processed within the VIS, the categories of persons to whom the data may be transmitted (recipients), and the data retention period. In addition, visa applicants must be informed of the fact that the collection of their personal data under VIS is mandatory for the examination of their application, while Member States must also inform them about the existence of their right to access their data, request their rectification or deletion, and about the procedures enabling them to exercise these rights.[877]

- The right to access the personal data related to them which have been recorded in the VIS.[878]

- The right to correct inaccurate data.[879]

- The right to delete unlawfully stored data.[880]

To ensure supervision of VIS, the VIS SCG was set up. It consists of representatives of the EDPS and the national supervisory authorities, which meet up twice a year. This group consists of the representatives of the 28 EU Member States and from Iceland, Liechtenstein, Norway and Switzerland.[881]

Eurodac

Eurodac stands for European Dactyloscopy. It is a centralised system that contains the fingerprint data of third-country nationals and stateless persons who apply

877 VIS Regulation, Art. 37.

878 *Ibid.*, Art. 38 (1).

879 *Ibid.*, Art. 38 (2).

880 *Ibid.*, Art. 38 (2).

881 See the European Data Protection Supervisor's webpage on Eurodac.

for asylum in one of the EU Member States.[882] The system has been in operation since January 2003, with the adoption of Council Regulation No. 2725/2000; a recast became applicable in 2015. Its purpose is primarily to assist in determining which Member State should be responsible for examining a particular asylum application under Regulation (EC) No. 604/2013. That regulation establishes the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (Dublin III Regulation).[883] Personal data in Eurodac mainly serve the purpose of facilitating the application of the Dublin III Regulation.[884]

National law enforcement authorities and Europol are allowed to compare fingerprints linked to criminal investigations with the fingerprints contained in Eurodac, but only for the purpose of preventing, detecting or investigating terrorist or other serious criminal offences. Since Eurodac has been designed as an instrument for supporting the implementation of the EU's asylum policy, and not as a law enforcement tool, law enforcement authorities have access to the database only in specific cases, under specific circumstances, and under strict conditions.[885] For further use of the data for law-enforcement purposes, the Data Protection Directive for Police and Criminal Justice Authorities applies, whereas data used for the main purpose of facilitating the Dublin III Regulation is protected under the General Data Protection Regulation. Further transfer of personal data obtained by a Member State or

882 Council Regulation (EC) No. 2725/2000 of 11 December 2000 concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention, OJ 2000 L 316; Council Regulation (EC) No. 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No. 2725/2000 concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention, OJ 2002 L 62 (Eurodac Regulations), Regulation (EU) No. 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No. 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ 2013 L 180, p. 1 (Eurodac Recast Regulation).

883 Regulation (EU) No. 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person, OJ 2013 L 180 (Dublin III Regulation).

884 Eurodac Recast Regulation, OJ 2013 L 180, p. 1, Art. 1 (1).

885 *Ibid.*, Art. 1 (2).

Europol pursuant to the Eurodac Recast Regulation to any third country, international organisation or private entity established in or outside the EU, is prohibited.[886]

Eurodac consists of a central unit, operated by eu-LISA, for storing and comparing fingerprints, and a system for electronic data transmission between Member States and the central database. Member States take and transmit the fingerprints of every person of at least 14 years of age who asks for asylum in their territory, and of every non-EU national or stateless person of at least 14 years of age who is apprehended for the unauthorised crossing of their external border. Member States may also take and transmit the fingerprints of non-EU nationals or stateless persons who are found staying within their territory without permission.

Even though any Member States can consult Eurodac and request comparisons with fingerprint data, only the Member State that has collected the fingerprints and has transmitted them to the central unit has the right to amend the data, by correcting, supplementing or erasing them.[887] The eu-LISA keeps records of all data processing to monitor data protection and to ensure data security.[888] The national supervisory authorities assist and advise the data subjects on the exercise of their rights.[889] Collection and transmission of fingerprint data is subject to judicial review by the national courts.[890] The EU Institutions Data Protection Regulation[891] and supervision by the EDPS apply to processing activities of the Central System, which is managed by eu-LISA concerning Eurodac.[892] If a person suffers damage as a result of an unlawful processing operation, or from any act that is incompatible with the Eurodac regulation, this person is entitled to compensation from the Member State responsible for the damage.[893] It should be stressed, however, that asylum seekers are a particularly vulnerable group of people who have often undertaken long and risky travel. Because of their vulnerability and the precarious situation they are often in while examination of their asylum application is pending, in practice, exercising their rights, including the right to compensation, may prove difficult.

886 *Ibid.*, Art. 35.

887 *Ibid.,* Art. 27.

888 *Ibid.*, Art. 28.

889 *Ibid.,* Art. 29.

890 *Ibid.,* Art. 29.

891 Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, OJ 2001 L 8.

892 Eurodac Recast Regulation, OJ 2013 L 180, p. 1, Art. 31.

893 *Ibid.*, Art. 37.

To use Eurodac for law enforcement purposes, Member States have to designate the authorities that will have the right to request access, as well as the authorities that will verify that the requests for comparison are lawful.[894] Access of national authorities, and of Europol, to the Eurodac fingerprint data is subject to very strict conditions. The requesting authority must submit a reasoned electronic request only after comparing the data with that in other available information systems, such as national fingerprint databases and the VIS. There has to be an overriding public security concern that renders the comparison proportionate. The comparison must be truly necessary, relate to a specific case and there must be reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls in a category that is subject to the collection of fingerprints within the Eurodac system. The comparison must be made solely with fingerprint data. Europol must also obtain authorisation from the Member State that collected the fingerprint data.

Personal data stored in Eurodac that relate to asylum applicants are kept for 10 years from the date on which the fingerprints were taken, unless the data subject obtains the citizenship of an EU Member State. In this case, the data must be immediately erased. Data relating to foreign nationals apprehended for unauthorised crossing of the external border are stored for 18 months. These data must be erased immediately if the data subject receives a residence permit, leaves EU territory or obtains the citizenship of a Member State. The data of the persons who were granted asylum remain available for comparison in the context of preventing, detecting and investigating terrorist and other serious criminal offences for three years.

In addition to all EU Member States, Iceland, Norway, Liechtenstein and Switzerland also apply Eurodac on the basis of international agreements.

The Eurodac SCG has been set up to ensure supervision of Eurodac. It consists of representatives of the EDPS and the national supervisory authorities, which meet up twice a year. This group consists of the representatives of the 28 EU Member States and those of Iceland, Liechtenstein, Norway and Switzerland.[895]

894 Roots, L. (2015), 'The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination', *Baltic Journal of European Studies Tallinn University of Technology*, Vol. 5, No. 2, pp. 108–129.

895 See the European Data Protection Supervisor's webpage on Eurodac.

Outlook

In May 2016, the Commission issued a proposal on a new recast Eurodac Regulation, as part of a reform aiming to improve the functioning of the Common European Asylum System (CEAS).[896] The proposed recast is important, as it will significantly extend the scope of the original Eurodac database. Eurodac was initially created to support the implementation of the CEAS, by providing fingerprint evidence to enable the determination of which Member State is responsible for examining an asylum application lodged in the EU. The proposed recast will extend the scope of the database to facilitate the return of irregular migrants.[897] National authorities will be able to consult the database for purposes of identifying third country nationals who stay in the EU irregularly, or who have entered the EU irregularly, in order to obtain evidence to assist Member States to return these individuals. In addition, while the legal regime currently in place only requires the collection and storage of fingerprints, the proposal introduces the collection of individuals' facial images,[898] which is another type of biometric data. The proposal would also lower the minimum age of children from whom the biometric data can be taken – to six years[899] instead of 14 years, which is the minimum age under the 2013 regulation. The extended scope of the proposal means that it will constitute an interference with the rights to privacy and the data protection of more individuals who may be included in the database. To counterbalance this interference, the proposal, and the amendments proposed

896 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), COM(2016) final, 4 May 2016.

897 See the explanatory memorandum to the proposal, p. 3.

898 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), COM(2016) final, 4 May 2016, Art. 2 (1).

899 *Ibid.*, Art. 2 (2).

by the European Parliament's LIBE Committee,[900] seek to reinforce data protection requirements. At the time of drafting of the handbook, discussions of the proposal in the Parliament and the Council were ongoing.

Eurosur

The European Border Surveillance System (Eurosur)[901] is designed to enhance the control of Schengen external borders by detecting, preventing and combating irregular immigration and cross-border crime. It serves to enhance information exchange and operational cooperation between national coordination centres and Frontex, the EU agency in charge of developing and applying the new concept of integrated border management.[902] Its general objectives are:

- to reduce the number of irregular migrants entering the EU undetected;
- to reduce the number of deaths of irregular migrants by saving more lives at sea;
- to increase the internal security of the EU as a whole by contributing to the prevention of cross-border crime.[903]

Eurosur started its work on 2 December 2013 in all Member States with external borders, and on 1 December 2014 in the others. The regulation applies to the surveillance of external land, sea and air borders of the Member States. Eurosur

900 European Parliament, *Report on the proposal for a regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast),* PE 597.620v03-00, 9 June 2017.

901 Regulation (EU) No. 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur), OJ 2013 L 295.

902 Regulation (EU) No. 2916/1624 of the European Parliament and of the Council of 14 September 2016on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No. 863.2007 of the European Parliament and of the Council, Council Regulation (EC) No. 2007/2004 and Council Decision 2005/267/EC, OJ L 251.

903 See also: European Commission (2008), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Examining the creation of a European Border Surveillance System (Eurosur),* COM(2008) 68 final, Brussels, 13 February 2008; European Commission (2011), *Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (Eurosur),* Staff working paper, SEC(2011) 1536 final, Brussels,12 December 2011, p. 18.

exchanges and processes personal data to a very limited extent, as Member States and Frontex are only entitled to exchange ship identification numbers. Eurosur exchanges operational information, such as the location of patrols and incidents, and as a general rule, the information exchanged cannot include personal data.[904] In the exceptional cases where personal data are being exchanged within the framework of Eurosur, the regulation provides that the general EU legal framework on data protection applies fully.[905]

Eurosur thus ensures the right to data protection, namely by stating that exchanges of personal data must comply with the criteria and safeguards set by the Data Protection Directive for Police and Criminal Justice Authorities and the General Data Protection Regulation.[906]

Customs Information System

Another important information system established at EU level is the Customs Information System (CIS).[907] In the course of establishing an internal market, all checks and formalities in respect of goods moving within the EU territory were abolished, leading to a heightened risk of fraud. This risk was counterbalanced by intensified cooperation between the Member States' customs administrations. The purpose of CIS is to assist the Member States in preventing, investigating and prosecuting serious violations of national and EU customs and agricultural laws. The CIS is established by two legal acts, adopted on different legal bases: Council Regulation (EC) No. 515/97 concerns the cooperation between the different national administrative authorities for combating fraud in the context of the customs union and the common agricultural policy, while Council Decision 2009/917/JHA aims to assist in the prevention, investigation and prosecution of serious contraventions of customs laws. This means that CIS is not just concerned with law enforcement.

The information contained in CIS comprises personal data related to commodities, means of transport, businesses, persons, goods and cash retained, seized or

904 European Commission, *EUROSUR: Protecting the Schengen external borders – protecting migrants' lives. EUROSUR in a nutshell*, 29 November 2013.

905 Regulation 1052/2013, Recital 13 and Art. 13.

906 *Ibid.*, Recital 13 and Art. 13.

907 Council of the European Union (1995), Council Act of 26 July 1995 drawing up the Convention on the use of information technology for customs purposes, OJ 1995 C 316, amended by Council of the European Union (2009), Regulation No. 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters, Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes, OJ 2009 L 323 (CIS Decision).

confiscated. The categories of data that can be processed are clearly defined, and include the names, nationality, sex, place and date of birth of the individuals concerned, the reason for the inclusion of their data in the system and the registration number of the means of transport.[908] This information may be used solely for the purposes of sighting, reporting or carrying out particular inspections or for strategic or operational analyses concerning persons suspected of breaching customs provisions.

Access to CIS is granted to the national customs, taxation, agricultural, public health and police authorities, as well as Europol and Eurojust.

The processing of personal data must comply with the specific rules established by Regulation No. 515/97 and Council Decision 2009/917/JHA, as well as the provisions of the General Data Protection Regulation, the EU Institutions Data Protection Regulation, Modernised Convention 108 and the Police Recommendation. The EDPS is responsible for supervising CIS's compliance with Regulation (EC) No. 45/2001. It convenes a meeting at least once a year with all national data protection supervisory authorities with competence regarding CIS-related supervisory issues.

Interoperability between EU information systems

Migration management, integrated border management of the EU's external borders and the fight against terrorism and cross-border crime pose important challenges and have become increasingly complex in a globalised world. In recent years, the EU has been working on a new comprehensive approach to safeguarding and maintaining security without compromising the EU's values and fundamental freedoms. In these efforts, effective information exchange amongst national law enforcement authorities, and between Member States and the relevant EU agencies, is key.[909] The existing EU information systems for border management and internal security have their respective objectives, institutional set-up, data subjects and users. The EU has been working on overcoming shortcomings in the functionalities of fragmented EU data management between the different information systems such as SIS II, VIS and

908 See CIS Decision, Art. 24, 25 and 28.

909 European Commission (2016), Communication from the Commission to the European Parliament and the Council: Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final, Brussels, 6 April 2016, European Commission (2016), Communication from the Commission to the European Parliament, the European Council and the Council: Enhancing Security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders, COM(2016) 602 final, Brussels, 14 September 2016, European Commission (2016), Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third-country nationals. See also, Communication from the Commission to the European Parliament, the European Council and the Council: Seventh progress report towards an effective and genuine Security Union, COM(2017) 261 final, Brussels, 16 May 2017.

Eurodac by exploring the potential for interoperability.[910] The main objective is to ensure that competent police, customs and judicial authorities systematically have the necessary information to perform their duties, while maintaining a balance with respect to the rights to privacy, data protection and other fundamental rights.

Interoperability is 'the ability of information systems to exchange data and to enable the sharing of information'.[911] This exchange must not compromise the necessarily strict rules on access and use guaranteed by the General Data Protection Regulation, the Data Protection Directive for Police and Criminal Justice Authorities, the EU Charter of Fundamental Rights and all other relevant rules. Any integrated solution for data management must not affect the principles of purpose limitation, data protection by design or data protection by default.[912]

In addition to improving the functionalities of the three main information systems – SIS II, VIS and Eurodac – the Commission has proposed the establishment of a fourth centralised border management system addressing third-country nationals: the Entry-Exit System (EES),[913] which is expected to be implemented by 2020.[914] The Commission has also issued a proposal on the establishment of a European Travel Information and Authorisation System (ETIAS),[915] a system that will gather information on persons travelling visa-free to the EU to allow for advance irregular migration and security checks.

910 Council of the European Union (2005), The Hague Programme: Strengthening Freedom, Security and Justice in the European Union, OJ 2005 C 53, European Commission (2010), Communication from the Commission to the European Parliament and the Council: Overview of information management in the area of freedom, security and justice, COM(2010) 385 final, European Commission (2016), Communication from the Commission to the European Parliament and the Council: Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final, Brussels, 6 April 2016, European Commission (2016), Commission Decision of 17 June 2016 setting up the High Level Expert Group on Information Systems and Interoperability, OJ 2016 C 257.

911 European Commission (2016), Communication from the Commission to the European Parliament and the Council: Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final, Brussels, 6 April 2016, p. 14.

912 *Ibid*., pp. 4–5.

913 European Commission (2016), Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No. 767/2008 and Regulation (EU) No. 1077/2011, COM(2016) 194 final, Brussels, 6 April 2016.

914 European Commission (2016), Communication from the Commission to the European Parliament and the Council: Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final, Brussels, 6 April 2016, p. 5.

915 European Commission (2016), Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No. 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624, COM(2016) 731 final, 16 November 2016.

9

Specific types of data and their relevant data protection rules

EU	Issues covered	CoE
General Data Protection Regulation Directive on privacy and electronic communications	**Electronic communications**	Modernised Convention 108 Telecommunication Services Recommendation
General Data Protection Regulation, Article 89	**Employment relations**	Modernised Convention 108 Employment Recommendation ECtHR, *Copland v. the United Kingdom*, No. 62617/00, 2007
General Data Protection Regulation, Article 9 (2) (h) and (i)	**Medical data**	Modernised Convention 108 Medical Data Recommendation ECtHR, *Z v. Finland*, No. 22009/93, 1997
Clinical Trials Regulation	**Clinical trials**	
General Data Protection Regulation, Article 6 (4), Article 89	**Statistics**	Modernised Convention 108 Statistical Data Recommendation
Regulation (EC) No. 223/2009 on European statistics CJEU, C-524/06, *Huber v. Bundesrepublik Deutschland* [GC], 2008	**Official statistics**	Modernised Convention 108 Statistical Data Recommendation

EU	Issues covered	CoE
Directive 2014/65/EU on markets in financial instruments Regulation (EU) No. 648/2012 on OTC derivatives, central counterparties and trade repositories Regulation (EC) No. 1060/2009 on credit rating agencies Directive 2007/64/EC on payment services in the internal market	Financial data	Modernised Convention 108 Recommendation 90 (19) used for payments and other related operations ECtHR, *Michaud v. France*, No. 12323/11, 2012

In several instances, special legal instruments have been adopted at European level to apply the general rules of Modernised Convention 108 or of the General Data Protection Regulation in more detail to specific situations.

9.1. Electronic communications

Key points

- Specific rules on data protection in the area of telecommunications, making particular reference to telephone services, are contained in the 1995 CoE Recommendation.
- The processing of personal data relating to the delivery of communications services at the EU level is regulated in the Directive on privacy and electronic communications.
- Confidentiality of electronic communications relates not only to the content of a communication but also to metadata, such as information about who communicated with whom, when and for how long, and location data, such as where the data were communicated from.

Communications networks have a heightened potential for unjustified interference with the personal sphere of the users, as they provide powerful technical possibilities for listening in on and surveying the communications performed on such networks. Consequently, special data protection regulations were deemed necessary to address the particular risks for users of communications services.

In 1995, the **CoE** issued a Recommendation for data protection in the area of telecommunications, with particular reference to telephone services.[916] According to this recommendation, the purposes of collecting and processing personal data in the context of telecommunications should be limited to: connecting a user to the

916 Council of Europe, Committee of Ministers (1995), Recommendation Rec(95)4 to member states on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, 7 February 1995.

network, making the particular telecommunications service available, billing, verifying, ensuring optimal technical operation and developing the network and service.

Special attention was also given to the use of communications networks for sending direct marketing messages. As a general rule, direct marketing messages may not be directed at any subscriber who has expressly opted out of receiving them. Automated call devices for transmitting pre-recorded advertising messages may be used only if a subscriber has given express consent. Domestic law shall provide for detailed rules in this area.

Within the **EU legal framework,** after a first attempt in 1997, the Directive on privacy and electronic communications was adopted in 2002 and amended in 2009. This was done with the purpose of complementing and tailoring the provisions of the previous Data Protection Directive to the telecommunications sector.[917]

The application of the Directive on privacy and electronic communications is limited to communication services in public electronic networks.

The Directive on privacy and electronic communications distinguishes three main categories of data generated in the course of a communication:

- the data constituting the content of the messages sent during communication – these data are strictly confidential;
- the data necessary for establishing and maintaining the communication – so-called metadata, referred to as "traffic data" in the directive – such as information about the communication parties, time and duration of the communication;
- within the metadata, there are data specifically relating to the location of the communication device, so-called location data – these data are at the same time

917 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ 2002 L 201 (Directive on privacy and electronic communications) as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ 2009 L 337.

data about the location of the users of the communication devices, particularly where users of mobile communication devices are concerned.

Traffic data may be used by the service provider only for billing and for technically providing the service. With the consent of the data subject, however, these data may be disclosed to other controllers offering added value services, such as giving information in relation to the user's location about the next metro station or pharmacy or the weather forecast for this location.

According to Article 15 of the e-Privacy Directive, other access to data about communications in electronic networks must fulfil the requirements for justified interference of the right to data protection as laid down in Article 8 (2) of the ECHR and confirmed by the EU Charter of Fundamental Rights in Articles 8 and 52. Such access might include access for the purpose of investigating crimes.

The 2009 amendments to the Directive on privacy and electronic communications[918] introduced the following:

- The restrictions on sending emails for direct marketing purposes were extended to short message services, multimedia messaging services and other kinds of similar applications; marketing emails are prohibited unless prior consent was obtained. Without such consent, only previous customers may be approached with marketing emails, if they have made their email address available and do not object.

- An obligation was placed on Member States to provide judicial remedies against violations of the ban on unsolicited communications.[919]

- Setting of cookies, software that monitors and records a computer user's actions, is no longer allowed without the computer user's consent. National law should

918 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ 2009 L 337.

919 See the amended directive, Art. 13.

regulate in more detail how consent should be expressed and obtained to offer sufficient protection.[920]

Where a data breach occurs as a result of unauthorised access, loss or destruction of data, the competent supervisory authority must be informed immediately. The subscribers must be informed where possible damage to them is the consequence of a data breach.[921]

The Data Retention Directive[922] required communication service providers to retain metadata. However, this directive was annulled by the CJEU (for more details, see Section 8.3).

Outlook

In January 2017, the European Commission adopted a new proposal for an e-Privacy Regulation to replace the old e-Privacy Directive. The aim would remain the protection of "fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data". At the same time, the new proposal is to ensure free movement of electronic communications data and electronic communications services within the Union.[923] Whilst the General Data Protection Regulation primarily addresses Article 8 of the EU Charter of Fundamental Rights, the proposed regulation aims to incorporate Article 7 of the Charter into EU secondary law.

The regulation would adapt the previous directive's provisions to new technologies and market reality and would build a comprehensive and consistent framework with the General Data Protection Regulation. In this sense, the e-Privacy Regulation

920 See *Ibid.*, Art. 5; see also Article 29 Working Party (2012), *Opinion 04/2012 on cookie consent exemption*, WP 194, Brussels, 7 June 2012.

921 See also Article 29 Working Party (2011), *Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments*, WP 184, Brussels, 5 April 2011.

922 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006 L 105.

923 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (COM(2017) 10 final), Art. 1.

would be *lex specialis* to the General Data Protection Regulation, tailoring it to electronic communications data that constitute personal data. The new regulation covers the processing of "electronic communications data", including electronic communications content and metadata that are not necessarily personal data. The territorial scope is limited to the EU, including when data obtained in the EU are processed outside it, and extends to over-the-top communications service providers. These are service providers that deliver content, services or applications over the internet, without the direct involvement of a network operator or internet service provider (ISP). Examples of such providers include Skype (voice and video calling), WhatsApp (messaging), Google (search), Spotify (music) or Netflix (video content). The enforcement mechanisms of the General Data Protection Regulation would apply to the new regulation.

The e-Privacy Regulation is intended to be adopted before 25 May 2018, by which time the General Data Protection Regulation will be applicable in all 28 Member States. However, this is conditional upon the agreement of both the European Parliament and the Council.[924]

9.2. Employment data

Key points

- Specific rules for data protection in employment relations are outlined in the CoE Employment Data Recommendation.
- In the General Data Protection Regulation, employment relations are specifically referred to only in the context of the processing of sensitive data.
- The validity of consent, which must have been freely given, as a legal basis for processing data about employees may be questionable, considering the economic imbalance between employer and employees. The circumstances surrounding consent must be assessed carefully.

924 For more information, see European Commission (2017), "Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions", press release, 10 January 2017.

Data processing in the context of employment is subject to the general EU legislation on the protection of personal data. However, one regulation[925] specifically deals with the protection of the processing of personal data by the European institutions in the context of employment (among other things). In the General Data Protection Regulation, employment relations are specifically referred to in Article 9 (2), which states that personal data may be processed when carrying out obligations or exercising the specific rights of the controller or the data subject in the field of employment.

Under the General Data Protection Regulation, the employee should be enabled to clearly distinguish the data to which he or she freely consents to being processed/stored and the purposes for which his or her data are stored. Employees should also be informed of their rights and the length of time the data will be stored, before consent can be given. Should a breach of personal data likely to result in a high risk to the rights and freedoms of natural persons occur, the employer must communicate this breach to the employee. Article 88 of the regulation permits Member States to establish more specific rules to ensure the protection of employees' rights and freedoms in respect of their personal data in the employment context.

> Example: In the *Worten* case,[926] the data included a record of working time containing the daily work and rest periods, which constitute personal data. National law may require an employer to make the records of working time available to the national authorities responsible for monitoring working conditions. This would allow immediate access to the relevant personal data. However, access to the personal data is necessary to allow the national authority to monitor the legislation on working conditions.[927]

As regards the **CoE**, the Employment Data Recommendation was issued in 1989 and revised in 2015.[928] The recommendation covers the processing of personal data for employment purposes in both private and public sectors. The processing must comply with certain principles and restrictions, such as the principle of transparency

925 Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001 L 8.

926 CJEU, C-342/12, *Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT)*, 30 May 2013, para. 19.

927 *Ibid.*, para. 43.

928 Council of Europe, Committee of Ministers (2015), Recommendation Rec(2015)5 to member states on the processing of personal data in the context of employment, April 2015.

and consulting employees' representatives before placing monitoring systems in the workplace. The recommendation also states that employers should apply preventative measures, such as filters, instead of monitoring employees' internet usage.

A survey of the most common data protection problems specific to the employment context can be found in a working document of the Article 29 Working Party.[929] The working party analysed the significance of consent as a legal basis for processing employment data.[930] It found that the economic imbalance between the employer asking for consent and the employee giving consent will often raise doubts about whether or not consent was given freely. The circumstances under which consent is relied on as the legal basis for data processing should therefore be carefully considered when assessing the validity of consent in the employment context.

A common data protection problem in today's typical working environment is the extent of monitoring employees' electronic communications legitimately within the workplace. It is often claimed that this problem can easily be solved by prohibiting private use of communication facilities at work. Such a general prohibition could, however, be disproportionate and unrealistic. The ECtHR's judgments in *Copland v. the United Kingdom* and *Bărbulescu v. Romania* are of particular interest in this context.

Example: In *Copland v. the United Kingdom*,[931] the telephone, email and internet usage of a college employee was secretly monitored to ascertain whether she was making excessive use of college facilities for personal purposes. The ECtHR held that telephone calls from business premises were covered by the notions of private life and correspondence. Therefore, such calls and emails sent from work, as well as information derived from the monitoring of personal internet usage, were protected by Article 8 of the ECHR. In the applicant's case, no provisions existed which regulated the circumstances under which employers could monitor employees' use of telephone, email and the internet. Therefore, the interference was not in accordance with the law. The Court concluded that there had been a violation of Article 8 of the ECHR.

929 Article 29 Working Party (2017), *Opinion 2/2017 on data processing at work*, WP 249, Brussels, 8 June 2017.

930 Article 29 Working Party (2005), *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, WP 114, Brussels, 25 November 2005.

931 ECtHR, *Copland v. the United Kingdom*, No. 62617/00, 3 April 2007.

Example: In *Bărbulescu v. Romania,*[932] the applicant was dismissed for using the internet at his place of employment during working hours, in breach of internal regulations. His employer monitored his communications. The records, showing messages of a purely private nature, were produced during the domestic proceedings. In finding Article 8 to be applicable, the ECtHR left open the question of whether the employer's restrictive regulations left the applicant with a reasonable expectation of privacy, but did find that an employer's instructions could not reduce private social life in the workplace to zero.

As regards the merits, Contracting States had to be granted a wide margin of appreciation in assessing the need to establish a legal framework governing the conditions in which an employer could regulate electronic or other communications of a non-professional nature by its employees in the workplace. Nevertheless, the domestic authorities had to ensure that the introduction by an employer of measures to monitor correspondence and other communications, irrespective of the extent and duration of such measures, was accompanied by adequate and sufficient safeguards against abuse. Proportionality and procedural guarantees against arbitrariness were essential and the ECtHR identified a number of factors which were relevant in the circumstances. These included, among others, the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy; the consequences for the employee; and whether adequate safeguards had been provided. In addition, domestic authorities had to ensure that an employee whose communications had been monitored had access to a remedy before a judicial body with jurisdiction to determine, at least in substance, how those criteria outlined were observed and whether the impugned measures were lawful.

In this case, the ECtHR found a violation of Article 8 because the domestic authorities had not afforded adequate protection of the applicant's right to respect for his private life and correspondence, and had consequently failed to strike a fair balance between the interests at stake.

According to the CoE Employment Recommendation, personal data collected for employment purposes should be obtained from the individual employee directly.

932 ECtHR, *Bărbulescu v. Romania* [GC], No. 61496/08, 5 September 2017, para. 121.

Personal data collected for recruitment must be limited to the information necessary to evaluate the suitability of candidates and their career potential.

The recommendation also specifically mentions judgmental data relating to the performance or potential of individual employees. Judgmental data must be based on fair and honest evaluations and must not be insulting in the way they are formulated. This is required by the principles of fair data processing and accuracy of data.

A specific aspect of data protection law in the employer–employee relationship is the role of employees' representatives. Such representatives may receive the personal data of employees only insofar as this is necessary to allow them to represent the interests of the employees or if such data are necessary to fulfil or supervise the obligations laid down in collective agreements.

Sensitive personal data collected for employment purposes may only be processed in particular cases and according to safeguards laid down by domestic law. Employers may ask employees or job applicants about their state of health or may examine them medically only where this is necessary. This may be to: determine their suitability for the employment; fulfil the requirements of preventative medicine; safeguard the vital interests of the data subject or other employees and individuals; allow social benefits to be granted; or respond to judicial requests. Health data may not be collected from sources other than the employee concerned, except when express and informed consent was obtained or when national law provides for this.

Under the Employment Recommendation, employees should be informed about the purpose of the processing of their personal data, the type of personal data collected, the entities to which the data are regularly communicated and the purpose and legal basis of such disclosures. Electronic communication may only be accessed in the workplace on the grounds of security or other legitimate reasons, and such access is only allowed after employees have been informed that the employer may have access to this kind of communication.

Employees must have a right of access to their employment data as well as a right to rectification or erasure. If judgmental data are processed, employees must, further, have a right to contest the judgment. These rights may, however, be temporarily limited for the purpose of internal investigations. If an employee is denied access, rectification or erasure of personal employment data, national law must provide appropriate procedures to contest such denial.

9.3. Health data

Key point

- Medical data are sensitive data and therefore enjoy specific protection.

Personal data concerning the health of the data subject qualify as sensitive data under Article 9 (1) of the General Data Protection Regulation and under Article 6 of Modernised Convention 108. Accordingly, health-related data are subject to a stricter data-processing regime than non-sensitive data. The General Data Protection Regulation prohibits the processing of "personal data concerning health" (understood as "all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject")[933], as well as genetic data and biometric data, unless it is authorised under Article 9 (2). Both types of data have been added to the list of "special categories of data".[934]

Example: In *Z v. Finland*,[935] the applicant's ex-husband, who was infected with HIV, had committed a number of sexual offences. He was subsequently convicted of manslaughter on the ground that he had knowingly exposed his victims to the risk of HIV infection. The national court ordered the full judgment and the case documents to remain confidential for 10 years despite requests from the applicant for a longer confidentiality period. The appellate court refused these requests, and its judgment contained the full names of both the applicant and her ex-husband. The ECtHR held that the interference was not considered necessary in a democratic society, because the protection of medical data was of fundamental importance to the enjoyment of the right to respect for private and family life, in particular when it came to information about HIV infections, given the stigma attached to this condition in many societies. Therefore, the Court concluded that allowing access to the appellate court's judgment, which described the applicant's identity and medical condition, as soon as 10 years after issuing the judgment would violate Article 8 of the ECHR.

933 General Data Protection Regulation, Recital 35.

934 *Ibid*., Art. 2.

935 ECtHR, *Z v. Finland*, No. 22009/93, 25 February 1997, paras. 94 and 112; see also ECtHR, *M.S. v. Sweden*, No. 20837/92, 27 August 1997; ECtHR, *L.L. v. France*, No. 7508/02, 10 October 2006; ECtHR, *I v. Finland*, No. 20511/03, 17 July 2008; ECtHR, *K.H. and Others v. Slovakia*, No. 32881/04, 28 April 2009; ECtHR, *Szuluk v. the United Kingdom*, No. 36936/05, 2 June 2009.

Under **EU law**, Article 9 (2) (h) of the General Data Protection Regulation allows for processing medical data where this is required for the purposes of preventative medicine, medical diagnosis, the provision of care or treatment, or the management of healthcare services. Processing is permissible, however, only where performed by a healthcare professional subject to an obligation of professional secrecy, or by another person subject to an equivalent obligation.[936]

Under **CoE law**, the CoE Medical Data Recommendation of 1997 applies the principles of Convention 108 to data processing in the medical field in more detail.[937] The proposed rules are in line with those of the General Data Protection Regulation as concerns the legitimate purposes of processing medical data, the necessary professional secrecy obligations of persons using health data, and the rights of the data subjects to transparency and access, rectification and deletion. Moreover, medical data which are lawfully processed by healthcare professionals may not be transferred to law enforcement authorities unless "sufficient safeguards to prevent disclosure inconsistent with the respect for [...] private life guaranteed under Article 8 of the ECHR" are provided.[938] The national law must also be "formulated with sufficient precision and afforded adequate legal protection against arbitrariness".[939]

Additionally, the Medical Data Recommendation contains special provisions on the medical data of unborn children and incapacitated persons, and on the processing of genetic data. Scientific research is explicitly acknowledged as a reason for conserving data longer than they are needed, although this will usually require anonymisation. Article 12 of the Medical Data Recommendation proposes detailed regulations for situations where researchers need personal data and anonymised data are insufficient.

Pseudonymisation may be an appropriate means to satisfy scientific needs and at the same time protect the interests of the patients concerned. The concept of pseudonymisation in the context of data protection is explained in more detail in Section 2.1.1.

936 See also ECtHR, *Biriuk v. Lithuania*, No. 23373/03, 25 November 2008.

937 Council of Europe, Committee of Ministers (1997), Recommendation Rec(97)5 to member states on the protection of medical data, 13 February 1997. Note that this Recommendation is in the process of being revised.

938 ECtHR, *Avilkina and Others v. Russia*, No. 1585/09, 6 June 2013, para. 53.

939 ECtHR, *L.H. v. Latvia*, No. 52019/07, 29 April 2014, para. 59.

The 2016 CoE Recommendation on data resulting from genetic tests also applies to data processing in the medical field.[940] This recommendation is of great importance to eHealth, where ICT is used to facilitate medical care. An example is sending a patient's parental test results from one healthcare provider to another. This recommendation aims to protect the rights of persons whose personal data are processed for insurance purposes to insure against risks related to a person's health, physical integrity, age or death. Insurers need to justify the processing of health-related data and it should be proportionate to the nature and importance of the risk being considered. The processing of this kind of data is dependent on the subject's consent. Insurers should also have safeguards in place for the storage of health-related data.

Clinical trials – which involve assessing the effects of new drugs on patients in documented research environments – have considerable data protection implications. Clinical trials of medical products for human use are regulated by Regulation (EU) No. 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (Clinical Trials Regulation).[941] The main elements of the Clinical Trials Regulation are:

- a streamlined application procedure via the EU portal;[942]
- deadlines for the assessment of the application for clinical trials;[943]
- an ethics committee being part of the assessment, in accordance with the law of the Member States (and European law defining the time periods involved);[944] and
- improved transparency of clinical trials and their outcomes.[945]

940 Council of Europe, Committee of Ministers (2016), Recommendation Rec(2016)8 to member states on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests, 26 October 2016.

941 Regulation (EU) No. 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (Clinical Trials Regulation), OJ 2014 L 158.

942 Clinical Trials Regulation, Art. 5 (1).

943 *Ibid*., Art. 5 (2)–(5).

944 *Ibid*., Art. 2 (11).

945 *Ibid*., Art. 9 (1) and Recital 67.

The General Data Protection Regulation specifies that for the purposes of consenting to participation in scientific research activities in clinical trials, Regulation (EU) No. 536/2014 applies.[946]

Many other legislative and other initiatives on personal data in the health sector are pending at EU level.[947]

Electronic health records

Electronic health records are defined as "a comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form, and providing for ready availability of these data for medical treatment and other closely related purposes".[948] Electronic health records are electronic versions of patients' medical history and may include clinical data relating to these individuals, such as past medical history, problems and conditions, medications and treatments, as well as exam and laboratory results and reports. These electronic files, which can vary from entire records to mere extracts or summaries, can be accessed by the general practitioner, pharmacist and other healthcare professionals. The concept of 'eHealth' also touches upon these health records.

Example: Mr. A has taken out an insurance policy with company B, the insurer. The latter will collect some health-related information from A, such as ongoing health issues or illnesses. The insurer should store A's health-related personal data separately from other data. The insurer also needs to store the health-related personal data separately from other personal data. This means that only A's case handler will have access to A's health-related data.

Nevertheless, certain data protection issues are raised by electronic health files, such as their accessibility, proper storage, and access by the data subject.

In addition to electronic health records, on 10 April 2014, the European Commission published a Green Paper on mobile health (mHealth), considering that mHealth is an

946 General Data Protection Regulation, Recitals 156 and 161.

947 EDPS (2013), *Opinion of the European Data Protection Supervisor on the Communication from the Commission on 'eHealth Action Plan 2012–2020 – Innovative healthcare for the 21st century*, Brussels, 27 March 2013.

948 Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems, Point 3 (c).

emerging and rapidly growing field that has the potential to transform healthcare and increase its efficiency and quality. The term covers medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants, and other wireless devices, as well as applications (for example, well-being applications) that may connect to medical devices or sensors.[949] The paper outlines the risks to the right to protection of personal data that the development of mHealth could entail, and provides that, given the sensitive nature of health data, the development should contain specific and suitable security safeguards for patient data, such as encryption, and appropriate patient authentication mechanisms to mitigate security risks. Compliance with personal data protection rules, including the obligation to provide information to the data subject, data security and the principle of lawful processing of personal data is vital for building trust in mHealth solutions.[950] To this end, a Code of Conduct has been drafted by the industry, based on inputs from a wide range of stakeholders, containing representatives with expertise in data protection, self- and co-regulation, ICT and health care.[951] At the time of drafting of the handbook, the draft code of conduct had been submitted for comments to the Article 29 Data Protection Working Party, pending its formal approval.

9.4. Data processing for research and statistical purposes

Key points

- Data collected for statistical, scientific or historical research purposes may not be used for any other purpose.
- Data collected legitimately for any purpose may be further used for statistical, scientific or historical research purposes, provided that adequate safeguards are in place. For this purpose, anonymisation or pseudonymisation before the transmission of data to third parties can provide these safeguards.

EU law allows for the processing of data for statistical and scientific or historical research purposes, provided that appropriate safeguards for the rights and freedoms

949 European Commission (20140), *Green paper on mobile Health ("mHealth")*, COM(2014) 219 final, Brussels, 10 April 2014.

950 *Ibid.*, p. 8.

951 Draft Code of Conduct on privacy for mobile health applications, 7 June 2016.

of the data subjects are in place. These may include pseudonymisation.[952] EU law or national law may provide for certain derogations from the rights of data subjects if these rights are likely to render impossible, or seriously impair, the achievement of the legitimate purpose of the research.[953] Derogations can be introduced from the right of access by the data subject, the right to rectification, the right to restriction of processing and the right to object.

Although data lawfully collected by a controller for any purpose may be re-used by this controller for their own statistical, scientific or historical research purposes, the data would have to be anonymised or subject to measures such as pseudonymisation, depending on the context, before transmitting them to a third party for statistical, scientific or historical research purposes, unless the data subject consented to it, or it is specifically provided for in national law. Data subject to pseudonymisation remain subject to the General Data Protection Regulation, unlike anonymous data.[954]

The regulation thus accords research special treatment in respect of the general data protection rules to avoid limitations to research development and to comply with the objective of achieving a European research area, as set out in Article 179 TFEU. It provides for the broad interpretation of the processing of personal data for scientific research purposes, including technological development and demonstration, basic research, applied research and privately funded research. It also recognises the importance of the compilation of data in registries for research purposes and the possible difficulty in fully identifying the subsequent purpose of personal data processing for scientific research purposes at the time of data collection.[955] For this reason, the regulation allows the processing of data for these purposes, without the data subjects' consent, provided the relevant safeguards are in place.

An important example of the use of data for statistical purposes are official statistics, obtained by the national and EU statistics bureaus pursuant to national and EU laws on official statistics. According to these laws, citizens and businesses are usually obliged to disclose data to the relevant statistics authorities. Officials working in statistics bureaus are bound by special professional secrecy obligations which must be complied with properly, as they are essential for the high-level of citizen trust necessary if data are to be made available to the statistics authorities.[956]

952 General Data Protection Regulation, Art. 89 (1).

953 *Ibid.*, Art. 89 (2).

954 *Ibid.*, Recital 26.

955 *Ibid.*, Recitals 33, 157 and 159.

956 *Ibid.*, Art. 90.

Regulation (EC) No. 223/2009 on European statistics (European Statistics Regulation) contains essential rules for data protection in the context of official statistics and may, therefore, also be considered relevant to provisions on official statistics made at the national level.[957] The regulation maintains the principle that official statistical activity needs a sufficiently clear legal basis.[958]

> Example: In *Huber v. Bundesrepublik Deutschland*,[959] an Austrian businessman who moved to Germany complained that the collection and storage of personal data of foreign nationals by German authorities in a central register (AZR) also for statistical purposes violated his rights under the Data Protection Directive. Considering that Directive 95/46 is intended to ensure an equivalent level of data protection in all Member States, the CJEU held that, to ensure a high level of protection in the EU, the concept of necessity in Article 7 (e) cannot have a meaning which varies among Member States. Thus, it is a concept which has its own independent meaning in EU law, and must be interpreted in a manner which fully reflects the objective of Directive 95/46. The CJEU, noting that only anonymous information should be required for statistical purposes, ruled that the German register was not compatible with the requirement of necessity under Article 7 (e).

In the context of the **CoE**, further processing of data can be carried out for scientific, historical or statistical purposes where this is in the public interest, and must be subject to appropriate safeguards.[960] Data subjects' rights may also be restricted when processing data for statistical purposes, provided that there is no recognisable risk of infringing their rights and freedoms.[961]

957 Regulation (EC) No. 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No. 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No. 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities, OJ 2009 L 87, as amended by Regulation (EU) 2015/759 of the European Parliament and of the Council of 29 April 2015 amending Regulation (EC) No. 223/2009 on European statistics, OJ 2015 L 123.

958 This principle is to be further detailed in Eurostat's Code of Practice, which shall, in accordance with Article 11 of the European Statistics Regulation, give ethical guidance on how to perform official statistics, including considerate use of personal data.

959 CJEU, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland* [GC], 16 December 2008; see especially para. 68.

960 Modernised Convention 108, Art. 5 (4) (b).

961 *Ibid.*, Art. 11 (2).

The Statistical Data Recommendation issued in 1997 covers the performance of statistical activity in the public and private sectors.[962]

Data collected by a controller for statistical purposes may not be used for any other purpose. Data collected for non-statistical purposes shall be available for further statistical use. The Statistical Data Recommendation also allows for the communication of data to third parties, provided this is for statistical purposes only. In such cases, the parties should agree and write down the extent of the legitimate further use for statistics. As this cannot replace the data subject's consent – if needed – there must be appropriate safeguards laid down in national law to minimise the risks of misusing personal data, such as an obligation to anonymise or pseudonymise the data before disclosure.

Statistical research professionals must be bound by special professional secrecy obligations – as is usually the case for official statistics – under national law. This must be extended also to interviewers and other collectors of personal data, if they are employed in collecting data from data subjects or other persons.

If a statistical survey using personal data is not authorised by law, the data subjects may have to consent to the use of their data to make it legitimate, or they may need to be given an opportunity to object. If personal data are collected for statistical purposes by interviewers, they must be informed clearly of whether or not providing data is mandatory under national law.

Where a statistical survey cannot be performed using anonymous data, and personal data are needed, the data collected for this purpose must be anonymised as soon as possible. The results of the statistical survey must not, at the least, allow for the identification of any data subjects, unless this would clearly present no risk.

After the statistical analysis has been concluded, the personal data used should either be deleted or anonymised. In cases like this, the Statistical Data Recommendation advises that identification data must be stored separately from other personal data. This means, for instance, that either the encryption key or the list containing the identifying synonyms must be stored separately to the other data.

962 Council of Europe, Committee of Ministers (1997), Recommendation Rec(97)18 to member states on the protection of personal data collected and processed for statistical purposes, 30 September 1997.

9.5. Financial data

Key points

- Although financial data are not considered sensitive data under Modernised Convention 108 or the General Data Protection Regulation, their processing requires particular safeguards to ensure accuracy and data security.
- Electronic payment systems particularly need built-in data protection, i.e. privacy or data protection by design and by default.
- Particular data protection problems can arise in this area because of the need to have appropriate authentication mechanisms in place.

Example: In *Michaud v. France*,[963] the applicant, a French lawyer, challenged his obligation under French law to report suspicions regarding possible money-laundering activities by his clients. The ECtHR observed that requiring lawyers to report information concerning another person, which had come into their possession through their professional exchanges, to the administrative authorities constituted an interference with the lawyers' right to respect for their correspondence and private life under Article 8 of the ECHR, as that concept covered activities of a professional or business nature. However, the interference was in accordance with the law and pursued a legitimate aim, namely the prevention of disorder and crime. Given that lawyers are subject to the obligation to report suspicious activity only under very specific circumstances, the ECtHR held that this obligation was proportionate. It concluded that there had not been a violation of Article 8.

Example: In *M.N. and Others v. San Marino,*[964] the applicant, an Italian citizen, concluded a fiduciary agreement with a company under investigation. This meant that the company was subject to the search and seizure of copies of (electronic) documentation. The applicant filed a complaint with the San Marino court, claiming that there was no link between him and the alleged crimes. However, the court declared his complaint inadmissible, as he was not an "interested party". The ECtHR held that the applicant had been at

963 ECtHR, *Michaud v. France*, No. 12323/11, 6 December 2012. See also ECtHR, *Niemietz v. Germany*, No. 13710/88, 16 December 1992, para. 29, and ECtHR, *Halford v. the United Kingdom*, No. 20605/92, 25 June 1997, para. 42.

964 ECtHR, *M.N. and Others v. San Marino*, No. 28005/12, 7 July 2015.

a significant disadvantage regarding judicial protection compared to an "interested party", yet his data were still subject to the search and seizure operations. Thus, the Court held that Article 8 was violated.

Example: In *G.S.B. v. Switzerland*,[965] the applicant's bank account details were sent to the US tax authorities on the basis of the administrative cooperation agreement between Switzerland and the US. The ECtHR held that transmission was not in violation of Article 8 ECHR because the interference with the applicant's right to privacy was prescribed by law, pursued a legitimate aim, and was proportionate to the public interest at stake.

Application of the general legal framework for data protection (as set out in Convention 108) to the context of payments, was developed by the **CoE** in Recommendation Rec(90)19 of 1990.[966] This recommendation clarifies the scope of the lawful collection and use of data in the context of payments, especially by means of payment cards. It also provides domestic legislators with detailed recommendations on the rules for disclosing payment data to third parties, on time limits for the retention of data, on transparency, data security and transborder data flows, and on supervision and remedies. The CoE has also developed an Opinion on the transfer of tax data,[967] which provides recommendations and issues to be taken into account when dealing with the transfer of tax data.

The ECtHR allows for the transmission of financial data – specifically, the details of an individual's bank account – under Article 8 ECHR, if it is prescribed by law, pursues a legitimate aim and is proportionate to the public interest at stake.[968]

In terms of **EU law**, electronic payment systems that involve the processing of personal data must comply with the General Data Protection Regulation. Therefore, these systems must ensure data protection by design and by default. Data protection by design obliges the controller to put appropriate technical and organisational measures in place to implement the data protection principles. Data protection by default means that the controller must ensure that only the personal data which

965 ECtHR, *G.S.B. v. Switzerland*, No. 28601/11 22 December 2015.

966 Council of Europe, Committee of Ministers (1990), Recommendation No. R(90)19 on the protection of personal data used for payment and other related operations, 13 September 1990.

967 Council of Europe, Consultative Committee of Convention 108 (2014), Opinion on the implication for data protection of mechanisms for automatic inter-state exchanges of data for administrative and tax purposes, 4 June 2014.

968 ECtHR, *G.S.B. v. Switzerland*, No. 28601/11, 22 December 2015.

are necessary for a specific purpose can be processed by default (see Section 4.4). Concerning financial data, the CJEU held that transferred tax data may constitute personal data.[969] The Article 29 Data Protection Working Party issued related guidelines for Member States, including criteria to ensure compliance with data protection rules when automatically exchanging personal data for tax purposes by automated means.[970] In addition, a number of legal instruments have been enacted to regulate the financial markets and the activities of credit institutions and investment firms.[971] Other legal instruments assist in fighting insider dealing and market manipulation.[972] The main areas that have an impact on data protection are:

- the retention of records of financial transactions;
- the transfer of personal data to third countries;
- the recording of telephone conversations or electronic communications, including the power of the competent authorities to request telephone and data traffic records;
- the disclosure of personal information, including the publication of sanctions;
- the supervisory and investigatory powers of the competent authorities, including on-site inspections and entering private premises to seize documents;
- the mechanisms for reporting breaches, i.e. whistle-blowing schemes; and

969 CJEU, C-201/14, *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others*, 1 October 2015, para. 29.

970 Article 29 Data Protection Working Party (2015), Statement of the WP29 on automatic inter-state exchanges of personal data for tax purposes, 14/EN WP 230.

971 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, OJ 2014 L 173; Regulation (EU) No. 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No. 648/2012, OJ 2014 L 173; Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, OJ 2013 L 176.

972 Regulation (EU) No. 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC, OJ 2014 L 173.

- the cooperation between competent authorities of Member States and the European Securities and Markets Authority (ESMA).

Other issues in these areas are also specifically addressed, including collecting data on the financial status of data subjects[973] or cross-border payment via banking transfers, which inevitably leads to personal data flows.[974]

973 Regulation (EC) No. 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies, OJ 2009 L 302, and most recently amended by Directive 2014/51/EU of the European Parliament and of the Council of 16 April 2014 amending Directives 2003/71/EC and 2009/138/EC and Regulations (EC) No. 1060/2009, (EU) No. 1094/2010 and (EU) No. 1095/2010 with respect to the powers of the European Supervisory Authority (European Insurance and Occupational Pensions Authority) and the European Supervisory Authority (European Securities and Markets Authority), OJ 2014 L 153; Regulation (EU) No. 462/2013 of the European Parliament and of the Council of 21 May 2013 amending Regulation (EC) No. 1060/2009 on credit rating agencies, OJ 2013 L 146.

974 Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ 2007 L 319, as amended by Directive 2009/111/EC of the European Parliament and of the Council of 16 September 2009 amending Directives 2006/48/EC, 2006/49/EC and 2007/64/EC regarding banks that are affiliated to central institutions, certain own-funds items, large exposures, supervisory arrangements, and crisis management, OJ 2009 L 302.

10 Modern challenges in personal data protection

The digital age, or information technology age, is characterised by the widespread use of computers, the internet and digital technologies. It involves the collection and processing of vast amounts of data, including personal data. The collection and processing of personal data in a globalised economy means that cross-border data flows are growing in number. Such processing can bring significant and visible benefits in everyday life: search engines facilitate access to considerable volumes of information and knowledge, social networking services enable people across the world to communicate, express opinions and mobilise support for social, environmental and political causes, while companies and consumers benefit from effective and efficient marketing techniques that boost the economy. Technology and personal data processing are also indispensable tools for state authorities in their fight against crime and terrorism. Similarly, big data – the collection, storage and analysis of large amounts of information to identify patterns and predict behaviour – "can be a source of significant value for society, enhancing productivity, public sector performance and social participation".[975]

Despite its multiple benefits, the digital age also poses challenges to privacy and data protection, as huge amounts of personal information are being collected and processed in increasingly complex and opaque ways. Technological progress has led to the development of massive data sets that can be easily cross-checked and further analysed to look for patterns, or for the adoption of decisions based on

975 Council of Europe, Consultative Committee of Convention 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, T-PD(2017)01, Strasbourg, 23 January 2017.

algorithms, which can provide unprecedented insight into human behaviour and private life.[976]

New technologies are powerful and can be particularly dangerous if they fall into the wrong hands. State authorities undertaking mass surveillance activities that may make use of these technologies are an example of the significant impact these technologies can have on the rights of individuals. In 2013, Edward Snowden's revelations on the operation of large-scale internet and phone surveillance programmes by intelligence agencies in some states sparked significant concerns about the dangers surveillance activities entail for privacy, democratic governance and freedom of expression. Mass surveillance and technologies allowing for globalised storage and processing of personal information and bulk access to data may impinge on the very essence of the right to privacy.[977] In addition, they can have a negative effect on political culture and a chilling effect on democracy, creativity and innovation.[978] The mere fear that the state may be constantly tracking and analysing the behaviour and actions of citizens can discourage them from expressing their views on certain matters and result in wariness and caution.[979] These challenges have prompted a number of public authorities, research centres and civil society organisations to analyse potential impacts of new technologies on society. In 2015, the European Data Protection Supervisor launched several initiatives aimed at assessing the impact of big data and the Internet of Things on ethics. Notably, it has set up an Ethics Advisory Group that aims to stimulate "an open and informed discussion on digital ethics, which allows the EU to realise the benefits of technology for society and the economy and at the same time reinforces the rights and freedoms of individuals, particularly their rights to privacy and data protection."[980]

Personal data processing is also a powerful tool in the hands of corporations. Today, it can reveal detailed information about a person's health or financial situation,

976 European Parliament (2017), Resolution on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law enforcement (P8_TA-PROV(2017)0076, Strasbourg, 14 March 2017.

977 See UN, General Assembly, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Ben Emmerson, A/69/397, 23 September 2014, para. 59. See also ECtHR, *Factsheet on Mass surveillance*, July 2017.

978 EDPS (2015), *Meeting the challenges of big data*, Opinion 7/2015, Brussels, 19 November 2015.

979 See notably CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [GC], 8 April 2014, para. 37.

980 EDPS, Decision of 3 December 2015 establishing an external advisory group on the ethical dimensions of data protection ('the Ethics Advisory Group'), 3 December 2015, Recital 5.

information then used by corporations to make important decisions for individuals, such as the health insurance premium to be applied to them or their creditworthiness. Data processing techniques may also have an impact on democratic processes, when used by politicians or corporations to influence elections – for instance, through the "micro-targeting" of voters' communications. In other words, while privacy was initially perceived as a right to protect individuals against unjustified interference by public authorities, in the modern era, it may also be threatened by the powers of private actors. This raises questions about the use of technology and predictive analysis in decisions that affect individuals' everyday lives, and reinforces the need to ensure that any personal data processing respects fundamental rights requirements.

Data protection is intrinsically connected to technological, social and political change. A comprehensive list of future challenges would therefore be impossible to devise. This chapter looks at select areas concerning big data, internet social networks and the EU's Digital Single Market. It is not an exhaustive assessment of these fields from a data protection perspective, instead highlighting the multitude of possible interactions between new or revised human activities and data protection.

10.1. Big data, algorithms and artificial intelligence

Key points

- Disruptive innovations in ICT are shaping a new way of life, where social relations, business, private and public services are digitally interconnected, thereby generating an increasingly large amount of data, many of which are personal data.
- Governments, enterprises and citizens increasingly operate in a data-driven economy, in which data themselves have become valuable assets.
- The concept of big data refers to both the data and analytics thereof.
- Personal data processed through big data analytics fall under EU and CoE legislation.
- Derogations from data protection rules and rights are limited to selected rights and to specific situations in which the enforcement of a right would prove impossible or would require disproportionate efforts by data controllers.
- Fully automated decision-making is generally prohibited, except in specific cases.
- Awareness among and control by individuals are key to ensuring rights enforcement.

In our increasingly digitised world, every activity leaves a digital trace that can be collected, processed and evaluated or analysed. With new information and communication technologies, more and more data are collected and recorded.[981] Until recently, no technology was able to analyse or evaluate the mass of data or to draw useful conclusions. The data were simply too numerous to evaluate, too complex, poorly structured and fast-moving to identify trends and habits.

10.1.1. Defining big data, algorithms and artificial intelligence

Big data

The term "big data" is a buzzword that may refer to several concepts, depending on the context. It commonly encompasses "the growing technological ability to collect process and extract new and predictive knowledge from great volume, velocity, and variety of data".[982] The concept of big data therefore covers both the data themselves and the data analytics.

The **sources** of the data are of various types, and include people and their personal data, machines or sensors, climate information, satellite imagery, digital pictures and videos, or GPS signals. A great deal of the data and information, however, are personal data – anything from a name, photo, email address, bank details, GPS tracking data, posts on social networking websites, medical information or a computer's IP address.[983]

Big data also refers to the **processing**, analysis and evaluation of the masses of data and available information, i.e. to gain useful information for the purposes of big data analysis. This means that the data and information collected can be used for

981 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions towards a thriving data economy COM(2014) 442 final, Brussels, 2 July 2014.

982 Council of Europe, Consultative Committee of Convention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 January 2017, p. 2; European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions towards a thriving data economy COM(2014) 442 final, Brussels, 2 July 2014, p. 4; International Telecommunications Union (2015), Recommendation Y.3600. Big Data – Cloud computing based requirements and capabilities.

983 EU Commission Fact Sheet on The EU Data Protection Reform and Big Data; Council of Europe, Consultative Committee of Convention 108 Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 January 2017, p. 2.

purposes than those originally intended, e.g. statistical trends, or more tailored services such as advertising. In fact, where the technologies do exist to collect, process and evaluate big data, any kind of information can be combined and re-evaluated: financial transactions, creditworthiness, medical treatment, private consumption, professional activity, tracking and routes taken, internet use, electronic cards and smartphones, video or communication monitoring. Big data analysis brings about a new quantitative dimension of data, one which can be evaluated and used in real-time, for example, to deliver tailored services to consumers.

Algorithms and artificial intelligence

Artificial intelligence (AI) refers to the intelligence of machines acting as "intelligent agents". As an intelligent agent, certain devices can, with the support of software, perceive their environment and take actions according to algorithms. The term AI is applied when a machine mimics "cognitive" functions – such as learning and problem solving – that would normally be associated with natural persons.[984] To mimic decision-making, modern technologies and software use algorithms which devices use to make "automated decisions". An algorithm is best described as a step-by-step procedure for calculation, data processing, evaluation and automated reasoning and decision-making.

Similarly to big data analytics, AI, and the automated decision-making it produces, requires the compilation and processing of large amounts of data. These data can come from the device itself (heat of the brakes, fuel, etc.) or from the surrounding environment. Profiling, for example, is a process that may rely on automated decision-making according to predetermined patterns or factors.

Example: Profiling and targeted advertising

Profiling based on big data involves looking for patterns that reflect "characteristics of a type of personality" – for example, when online shopping companies propose products "you may also like" based on information gathered from the products previously placed into a customer's shopping cart. The more data, the clearer the mosaic. The smartphone, for example,

984 Stuart Russel and Peter Norvig, *Artificial Intelligence: A Modern Approach (2nd ed.)*, 2003, Upper Saddle River, New Jersey: Prentice Hall, pp. 27, 32–58, 968–972; Stuart Russel and Peter Norvig, *Artificial Intelligence: A Modern Approach (3rd ed.)*, 2009, Upper Saddle River, New Jersey: Prentice Hall, p. 2.

is a powerful questionnaire which individuals complete with each use, consciously and unconsciously.

Modern psychography – the science of studying personalities – uses the OCEAN method, on the basis of which it determines the types of character dealt with. The 'Big Five' character dimensions relate to Openness (how open the person is to newness), Conscientiousness (how akin to a perfectionist the person is), Extraversion (how sociable the person is), Agreeableness (how agreeable the person is) and Neuroticism (how vulnerable the person is). This information profiles the person in question, their needs and fears, how they will behave, etc. It is then complemented by other information about the person, gained from any available sources, from data brokers, social networks (including the "likes" on posts and the photos posted), to music listened online, or GPS and tracking data.

The mass of profiles that are created through big data analysis techniques are subsequently compared to identify similar patterns and to construe clusters of personalities. The information about behaviour and attitudes of certain personalities is, therefore, inverted. With access to and use of big data, the personality test is turned around, with information about behaviour and attitude now used to describe the personality of the individual. By having the combined information about "likes" in social networks, tracking data, music listened to or movies watched, a clear picture can emerge of the personality of an individual, allowing businesses to communicate tailored advertising and/or information according to the "personality" of that person. Above all, this information can be processed in real-time.[985]

10.1.2. Balancing the benefits and risks of big data

Modern processing techniques can handle large masses of data, quickly import new ones, provide for real-time processing of the information in terms of short response time (even in the case of complex requests), provide for the possibility of multiple and simultaneous requests, and can analyse different types of information (photos, texts or numbers). These technological innovations make it possible

985 Processing techniques and new software evaluate the information about what a person likes, looks at when online shopping or adds to an online shopping cart in real-time and can propose "products" that might be of interest based on the information gathered.

to structure, process and evaluate masses of data and information in real-time.[986] By exponentially increasing the amount of data available and analysed, results that would be impossible in a smaller-scale analysis can now be achieved. Big data has helped develop a new field of business, in which new services may emerge for businesses and consumers alike. The value of EU citizens' personal data has the potential to grow to nearly EUR 1 trillion annually by 2020.[987] Therefore, big data may offer new **opportunities** resulting from the evaluation of mass data for new social, economic or scientific insights that can benefit individuals as well as businesses and governments.[988]

Big data analytics can reveal patterns between different sources and data sets, enabling useful insights in areas like science and medicine. This is the case, for example, in fields such as health, food security, intelligent transport systems, energy efficiency or urban planning. This real-time analysis of information can be used to improve the systems implemented. In research, new insights can be gained by combining large amounts of data and statistical evaluations, especially in disciplines in which a great deal of data have, until today, only been evaluated manually. New treatments can be developed, tailored to individual patients, based on comparisons with the mass of information available. Companies hope that the analysis of big data will enable them to gain competitive advantage, generate potential savings and create new business areas through direct, individualised customer service. Government agencies hope to achieve improvements in criminal justice. The Commission's Digital Single Market Strategy for Europe recognises the potential of

986 The development of software for the processing of Big Data is still in an early phase. Nevertheless, analytical programmes have recently been developed, especially for the analysis of mass data and information in real time, relating to activities of individuals. The possibility of analysing and processing Big Data in a structured way has provided new means of profiling and targeted advertising. European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions towards a thriving data economy COM(2014) 442 final, Brussels, 2 July 2014; EU Commission Fact Sheet on The EU Data Protection Reform and Big Data and Council of Europe, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 January 2017, p. 2.

987 EU Commission Fact Sheet on EU Data Protection Reform and Big Data.

988 International Conference of Data Protection and Privacy Commissioners (2014), Resolution on Big Data and European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions towards a thriving data economy COM(2014) 442 final, Brussels, 2 July 2014, p. 2; EU Commission Fact Sheet on EU Data Protection Reform and Big Data and Council of Europe, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 January 2017, p. 1.

data-driven technologies, services and big data to act as a catalyst for economic growth, innovation and digitisation in the EU.[989]

However, big data also carries **risks**, generally associated with its "three Vs" attributes: volume, velocity and variety of the data processed. The volume refers to the amount of data processed, variety to the number and diversity of types of data, while velocity refers to the speed of data processing. Specific considerations for data protection arise notably when big data analytics are used on large sets of data to extract new and predictive knowledge for decision-making purposes concerning individuals and/or groups.[990] The risks for data protection and privacy related to big data have been highlighted in Opinions of the EDPS and the Article 29 Working Party, resolutions of the European Parliament and in Council of Europe policy documents.[991]

Risks may include the mishandling of big data by those with access to the mass of information through manipulation, discrimination or oppression of individuals or specific groups in society.[992] Where masses of personal data or information about individual behaviour are collected, processed and evaluated, their exploitation can lead to significant violations of fundamental rights and freedoms going beyond the right to privacy. Measuring exactly the extent to which privacy and personal data may be affected is not possible. The European Parliament identified a lack of methodology to make an evidence-based assessment of the total impact of big data, but there is evidence to suggest that big data analytics can have a significant horizontal impact across both the public and private sector.[993]

989 European Parliament resolution of 14 March 2017 on fundamental rights implications of Big Data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225 (INI)).

990 Council of Europe, Consultative Committee of Convention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 January 2017, p. 2.

991 See, for example, EDPS (2015), *Meeting the Challenges of big data*, Opinion 7/2015, 19 November 2015; EDPS (2016), *Coherent enforcement of fundamental rights in the age of Big Data*, Opinion 8/2016, 23 September 2016; European Parliament (2016), Resolution on fundamental rights implications of Big Data: privacy, data protection, non-discrimination, security and law enforcement, P8_TA(2017)0076, Strasbourg, 14 March 2017; Council of Europe, Consultative Committee of Convention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, T-PD(2017)01, Strasbourg, 23 January 2017.

992 International Conference of Data Protection & Privacy Commissioners (2014), Resolution on Big Data.

993 European Parliament resolution of 14 March 2017 on fundamental rights implications of Big Data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI)).

The General Data Protection Regulation includes provisions on the right not to be subject to automated decision-making, including profiling.[994] The privacy issue arises where the exercise of the right to object requires human intervention, allowing data subjects to express their point of view and to contest the decision.[995] This can give rise to challenges in ensuring an adequate level of protection for personal data if, for example, no human intervention is possible or where the algorithms are too complex and the amount of data involved is too big to provide individuals with justifications for certain decisions, and/or prior information to obtain their consent. An example of the use of AI and automated decision-making is found in recent developments in mortgage applications or during recruiting processes. Applications are refused or turned down based on the fact that the applicants do not meet predetermined parameters or factors.

10.1.3. Data protection-related issues

In terms of data protection, the main issues concern, on the one hand, the volume and variety of personal data processed, and on the other hand, the processing and its results. The introduction of complex algorithms and software to transform mass data into a resource for decision-making purposes affects individuals and groups in particular, notably in cases of profiling or labelling, and ultimately raises many data protection issues.[996]

The identification of controllers and processors, and their liability

Big data and AI raise several questions in relation to the identification of controllers and processors, and their liability: when such a large amount of data is collected and processed, who is the owner of the data? When data are processed by intelligence machines and software, who is the controller? What are the exact responsibilities of each actor in the processing? And for what purposes may big data be used?

The question of liability in the context of AI will become all the more challenging when an AI takes a decision grounded on data processing it has developed itself. The General Data Protection Regulation provides a legal framework for the liability of data controller and processor. Unlawful processing of personal data gives rise

994 General Data Protection Regulation, Art. 22.

995 *Ibid.*, Art. 22 (3).

996 Council of Europe, Consultative Committee of Convention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 January 2017, p. 2.

to liability for the data controller and the data processor.[997] Artificial intelligence and automated decision-making raise questions about who is liable for violations affecting the privacy of data subjects where the complexity and amount of processed data cannot be ascribed with certainty. Where AI and algorithms are considered as products, this raises issues between personal liability, which is regulated under the General Data Protection Regulation, and product liability, which is not.[998] This would require rules on liability to fill the gap between personal liability and product liability for robotics and AI, including automated decision-making, for example.[999]

Impact on data protection principles

The nature, analysis and use of big data described above challenge the application of some of the traditional, fundamental principles of European data protection law.[1000] Such challenges mainly relate to the principles of lawfulness, data minimisation, purpose limitation, and transparency.

The principle of data minimisation requires personal data to be adequate, relevant and limited to what is necessary for the purposes for which they are processed. However, big data's business model may be the antithesis of data minimisation, as it requires more and more data, often for unspecified purposes.

The same applies to the principle of purpose limitation, which requires that data must be processed for specified aims, and cannot be used for purposes that are incompatible with the initial purpose of collection, unless such processing is based on a legal ground – such as, but not limited to, consent of the data subject (see Section 4.1.1).

Finally, big data also challenges the principle of accuracy of data, as big data applications tend to collect data from a variety of sources without having the possibility to check and/or maintain the accuracy of the data collected.[1001]

997 General Data Protection Regulation, Art. 77–79 and Art. 82.

998 European Parliament, European Civil Law Rules in Robotics, Directorate-General for Internal Policies, (October 2016), p. 14.

999 Speech of Roberto Viola at the Media seminar on European Law on Robotics at the European Parliament. (SPEECH 16/02/2017); European Parliament announcement on the request to the Commission for a proposal on Civil liability Rules for robotics and AI.

1000 Council of Europe, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD (2017) 01, Strasbourg, 23 January 2017.

1001 EDPS (2016), *Coherent enforcement of fundamental rights in the age of Big Data*, Opinion 8/2016, 23 September 2016, p. 8.

Specific rules and rights

The general rule remains that personal data being processed through big data analytics fall under the scope of data protection legislation. Specific rules or derogations for specific cases in relation to algorithmic complex data processing have nevertheless been introduced in EU and CoE law.

In CoE law, Modernised Convention 108 grants new rights to the data subject to enable a more effective control on his or her personal data in the big data era. It is precisely the case for instance with Article 1(a), (c) and (d) of Modernised Convention on the right not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration; the right to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her as well as the right to object. Other provisions of Modernised Convention 108, notably on transparency and additional obligations are complementary elements of the protective mechanism established with Modernised Convention 108 to tackle digital challenges.

In EU law, aside from cases listed in Article 23 of the GDPR, **transparency** must be ensured for all processing of personal data. It is especially important in relation to internet services and other complex automated data processing, such as the use of algorithms for decision-making. Here, the features of data processing systems must make it possible for data subjects to really understand what is happening with their data. To ensure fair and transparent processing, the General Data Protection Regulation requires the controller to provide the data subject with meaningful information about the logic involved in automated decision-making, including profiling.[1002] In its Recommendation on the protection and promotion of the right to freedom of expression and the right to private life, in respect of network neutrality, the Committee of Ministers of the Council of Europe recommended that internet service providers "provide users with clear, complete and publicly available information with regard to any traffic management practices which may affect users' access to and distribution of content, applications or services".[1003] Reports on internet traffic management practices, drawn up by competent authorities in all Member States, should

1002 General Data Protection Regulation, Art. 13 (2) (f).

1003 Council of Europe, Committee of Ministers (2016), Recommendation CM/Rec(2016)1 of the Committee of Ministers to the member states on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality, 13 January 2016, para. 5.1.

be prepared in an open and transparent manner and should be made available to the public free of charge.[1004]

Data controllers must **inform** data subjects – either when the data were collected from them or when they were not – not only of specific information on the data collected and the processing envisaged (see Section 6.1.1), but also, where relevant, of the existence of automated decision-making processes, providing them with "meaningful information about the logic involved",[1005] the objectives and the potential consequences of such processes. The General Data Protection Regulation also clarifies (only in cases where personal data have not been obtained from the data subject), that the controller is not obliged to provide the data subject with such information when "the provision of such information would prove impossible or would involve a disproportionate effort".[1006] However, as emphasised by the Article 29 Working Party in its *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679,* the complexity of the processing should not, in itself, preclude the data controller form providing data subject with clear explanations on the objectives and analytics used in the data processing.[1007]

Data subjects' rights to **access**, **rectify** and **erase** their personal data, as well as their right to **restrict** the processing, do not include a similar exemption. However, the obligation for the data controller to notify the data subject of any rectification or erasure of their personal data (see Section 6.1.4) may also be lifted when such notification would "prove impossible or involves a disproportionate effort".[1008]

Data subjects also have a right to **object**, as per Article 21 of the GDPR (see Section 6.1.6), to any processing of their personal data, including in cases of big data analytics. Whilst data controllers may be exempted from this obligation if they can demonstrate overriding legitimate interests, they may not enjoy such exemption in processing for direct marketing purposes.

1004 *Ibid.*, para. 5.2.

1005 General Data Protection Regulation, Art. 13 (2) f and 14 (2) g.

1006 *Ibid.*, Art. 14 (5) b.

1007 Article 29 Working Party, *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*, wp251, 3 October 2017, p. 14.

1008 General Data Protection Regulation, Art. 19.

Specific derogations to these rights may also be raised by data controllers when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[1009]

In relation to **profiling and automated decision-making**, the GDPR has introduced specific rules: Article 22 (1) stipulates that data subject "shall have the right not to be subject to a decision based solely on automated processing, which produces legal effects concerning him or her". As underlined by the Article 29 Working Party guidelines, this article states a general prohibition on fully automated decision-making.[1010] Data controllers may be exempted from such prohibition only in three specific cases: when the decision is: 1) necessary for the performance of a contract between the data subject and the controller, 2) permitted by an EU or national law, or 3) based on explicit consent.[1011]

Individual control

The complexity of, and lack of transparency around, big data analytics may require rethinking ideas of individual control of personal data. This should be tailored to the given social and technological context, taking into account the lack of knowledge on the part of individuals. Therefore, data protection in relation to big data should adopt a broader idea of control over the use of data, according to which individual control evolves into a more complex process of multiple impact assessments of the risks related to the use of data.[1012]

How good a big data application is depends on how well it can predict the desires or behaviour of test individuals (or consumers). Present prediction models based on big data analytics are constantly being refined. Recent developments include not only using data to categorise personalities (i.e. the behaviour and attitudes) but analysing behaviour through analysing voice patterns and the intensity with which messages are typed, or body temperature. All of this information can be used in real-time against the knowledge drawn from big data evaluations to assess creditworthiness during a meeting with a bank representative, for example. The assessment is

1009 *Ibid.*, Art. 89 (2) and (3).

1010 Article 29 Working Party, *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*, wp251, 3 October 2017, p. 9.

1011 General Data Protection Regulation, Art. 22 (2).

1012 Council of Europe, Consultative Committee of Convention 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD(2017)01, Strasbourg, 23 January 2017.

not made on the merits of the individual applying for the credit, but rather on the behavioural characteristics drawn from analysis and evaluation of big data information, i.e. the candidate speaking with a strong voice or flattering voice, his or her body language or body temperature.

Profiling and targeted advertising may not necessarily be a problem if individuals are **aware** that they are subject to tailored adverts. Profiling becomes a problem when it is used to manipulate individuals, i.e. to search for certain personalities or groups of people for political campaigning. For example, groups of undecided voters can be addressed via political messages tailored to their "personality" and attitudes. Another issue could be the use of such profiling to refuse access to goods and services to certain individuals. One safeguard that can provide protection against abuse of big data and personal information is pseudonymisation (see Section 2.1.1).[1013] Where personal data are truly anonymised, i.e. there is no information leaving traces connecting to the data subject, these cases fall outside the scope of the General Data Protection Regulation. Consent of data subjects and individuals in big data processing also presents a challenge for data protection law. This covers consent to being subject to tailored advertisements and profiling, which may be justified for "customer experience" reasons, and consent to the use of masses of personal data to refine and develop information-based, analytical tools. The awareness, or absence of awareness, of the big data processing raises several questions in relation to the means by which data subjects can exercise their rights, given that big data processing can rely on both pseudonymised and anonymised information subject to algorithms. While pseudonymised data fall under the General Data Protection Regulation, the regulation does not apply to anonymised data. Individual control on, and awareness of, their personal data processing is crucial in big data analytics: without it, they will not have a clear idea of who the data controller or processor is, preventing them to effectively exercise their rights.

10.2. The webs 2.0 and 3.0: social networks and Internet of Things

Key points

- Social Networking Services (SNS) are online communication platforms that enable individuals to join or create networks of like-minded users.

1013 *Ibid.*, p. 2.

- The Internet of Things is the connection of objects to the internet, and the interconnection of objects among themselves.
- Data subjects' consent is the most common legal basis for lawful data processing by data controllers on social networks.
- Social network users are generally protected by the "household exemption"; however, this derogation may be lifted in specific contexts.
- Providers of social networks are not protected by the "household exemption".
- Privacy by design and by default are crucial to ensure data security in this field.

10.2.1. Defining webs 2.0 and 3.0

Social Networking Services

Initially, the internet was conceived as a network to interconnect computers and to transmit messages with limited capabilities to exchange data, with websites merely offering the possibility for individuals to passively view their content.[1014] In the Web 2.0 era, the internet was transformed into a forum where users interact, collaborate and generate input. This era is characterised by the remarkable success and widespread use of social networking services, which are now an essential part of the everyday lives of millions of people.

Social Networking Services (SNS) or "social media" may be broadly defined as "online communication platforms enabling individuals to join or create networks of like-minded users".[1015] To join or create a network, individuals are invited to provide personal data and create their profile. SNS enable users to generate digital "content", ranging from photographs and videos to newspaper links and personal posts to express their views. Through these online communication platforms, users can interact and communicate with several other users. Importantly, most of the popular SNS do not require any registration fees. Rather than requiring users to pay to join the network, SNS providers generate most of their revenue from targeted advertising. Advertisers can benefit greatly from the personal information revealed daily on these sites. Having information on a user's age, gender, location and interests enables them to reach the "right" people with their ads.

1014 European Commission (2016), *Advancing the Internet of Things in Europe*, SWD(2016) 110 final.

1015 Article 29 Working Party (2009), *Opinion 5/2009 on online social networking*, WP 163, 12 June 2009, p. 4.

The Committee of Ministers of the Council of Europe adopted a Recommendation on the protection of human rights regarding social networking services,[1016] which in a specific section deals with data protection and was complemented in 2018 by another Recommendation on the roles and responsibilities of internet intermediaries.[1017]

Example: Nora is very happy because her partner proposed marriage. She wants to share the good news with her friends and family and decides to write an emotional post on a social network expressing her joy, and to change her relationship status to "engaged". In the coming days, when she logs into her account, Nora sees ads about wedding dresses and flower shops. Why is this so?

When creating an ad on Facebook, the wedding dress and flower companies selected certain parameters to be able to reach people like Nora. When Nora's profile indicates that she is a woman, engaged, living in Paris, close to the area the dress and flower shops placing the ads are located, she immediately sees the ads.

The Internet of Things

The Internet of Things (IoT) represents the next step in the development of the internet: the Web 3.0 era. With the IoT, devices may be connected and interact with other devices through the internet. This enables objects and people to be interconnected through communication networks, to report about their status and/or about the status of the surrounding environment.[1018] The IoT and connected devices are already a reality and are expected to grow substantially in the next few years, with the creation and further development of smart devices that will lead to the creation of smart cities, smart homes and smart businesses.

1016 Council of Europe, Committee of Ministers, Recommendation CM/Rec(2012)4 of the Committee of Ministers to member states on the protection of human rights with regard to social networking services, 4 April 2012.

1017 Council of Europe, Committee of Ministers, Recommendation CM/Rec(2018)2 of the Committee of Ministers to member states on the roles and responsibilities of internet intermediaries, 7 March 2018.

1018 European Commission, Commission Staff Working Document, *Advancing the Internet of Things in Europe*, SWD(2016) 110, 19 April 2016.

Example: IoT can be particularly beneficial for healthcare. Companies have already created devices, sensors and applications that allow for the monitoring of a patient's health. Through using a wearable alarm button and other wireless sensors place around the home, it is possible to track the daily routine of elderly people living alone and to generate alerts if serious disruptions are detected in their daily schedule. Fall detection sensors, for example, are widely used by older people. These sensors may detect falls with accuracy, and notify the individual's doctor and/or family about the fall.

Example: Barcelona is one of the most well-known examples of a smart city. Since 2012, the city has implemented the use of innovative technologies, aiming to create a smart system of public transit, waste management, parking and street lighting. To improve waste management, for example, the city uses smart bins. These enable the monitoring of waste levels to optimise collection routes. When bins are nearly full, they transmit signals via the mobile communications network which are sent to the software application used by the waste management company. The company can thus plan the best route for waste collection, prioritising and/or only arranging pick-ups for the bins that actually need to be emptied.

10.2.2. Balancing benefits and risks

The vast expansion and success of SNS in the past decade suggests that they have **significant benefits**. For instance, targeted advertising (as described in the highlighted example) is a particularly innovative way for companies to reach their audience, offering them a more specific market. It might also be in the interest of consumers to have ads presented to them that are more relevant and interesting. More importantly though, social networking services and social media can have a positive impact on society and on implementing change. They empower users to communicate, interact, organise groups and events on issues that affect them.

Similarly, the IoT is expected to bring significant benefits to the economy and is part of the EU strategy to develop a Digital Single Market. Within the EU, it is estimated that in 2020 the number of IoT connections will increase to six billion. This expansion of connectivity is expected to bring important economic benefits, through the development of innovative services and applications, better healthcare, better understanding of the needs of consumers and increased efficiency.

At the same time, given the huge amount of personal information generated by social media users and subsequently processed by the service operators, the expansion of SNS comes with a **growing concern** about the ways in which privacy and personal data can be protected. SNS may threaten the right to private life and the right to freedom of expression. Such threats may include: "lack of legal, and procedural, safeguards surrounding processes that can lead to the exclusion of users; inadequate protection of children and young people against harmful content or behaviours; lack of respect for others' rights; lack of privacy-friendly default settings; lack of transparency about the purposes for which personal data are collected and processed".[1019] European data protection law has tried to respond to the privacy/data protection challenges brought about by social media. Principles such as consent, privacy/data protection by design and by default, and the rights of individuals are particularly important in the context of social media and networking services.

In the context of IoT, the vast volume of personal data generated from the various interconnected devices also entails risks for privacy and data protection. While transparency is an important principle of European data protection law, due to the multitude of connected devices it is not always clear who is able to collect, access and use the data collected from IoT devices.[1020] However, under EU and CoE law, the transparency principle establishes an obligation for controllers to keep the data subjects informed about how their data are being used, in clear and plain language. The risks, rules, safeguards and rights in respect of the processing of their personal data must be made clear to the individuals concerned. IoT connected devices and the multiple processing operations and data involved could also challenge the requirement for clear and informed consent to data processing – when such processing is based on consent. Individuals often lack understanding of the technical functioning of such processing, and, therefore, of the consequences of their consent.

Another major concern is security, given that connected devices are particularly vulnerable to security risks. Connected devices have varying levels of security. As they operate beyond the standard IT infrastructure, they may lack the adequate processing power and storage capability to host security software or employ techniques such as encryption, pseudonymisation or anonymisation to protect users' personal information.

1019 Council of Europe, Recommendation Rec(2012)4 to member states on the protection of human rights with regard to social networking services, 4 April 2012.

1020 European Data Protection Supervisor (2017), *Understanding the Internet of Things*.

Example: In Germany, regulators decided to ban a toy connected to the internet following strong concerns about the toy's impact on the respect for the private life of children. Regulators considered that an internet-connected doll named Cayla effectively constituted a hidden spying device. The doll functioned by sending the audio questions of the child playing with it to an app on a digital device, which translated it into text and searched the internet for an answer. The app then sent a response to the doll, who voiced it to the child. Through this doll, the child's communications, as well as those of nearby adults, could be recorded and transmitted to the app. Had the doll manufacturers not adopted adequate security measures, the doll could have been used by anyone to listen to the conversations.

10.2.3. Data protection-related issues

Consent

In Europe, the processing of personal data is lawful only if it is permitted under European data protection law. For SNS providers, the consent of the data subjects generally provides a lawful basis for data processing. Consent must be given freely and be specific, informed and unambiguous (see Section 4.1.1).[1021] 'Freely given' essentially means that data subjects must have the ability to exercise a real and genuine choice. Consent is 'specific' and 'informed' where it is intelligible, referring clearly and precisely to the full scope, purposes and consequences of the data processing. In the context of social media, whether consent is free, specific and informed for all types of processing carried out by the SNS operator and third parties can be questioned.

Example: To join and access an SNS, individuals often have to agree to different kinds of processing of their personal data, often without being provided with the necessary specifications, or alternative options. An example would be the need to consent to receiving behavioural advertising to register with a SNS. As the Article 29 Working Party notes in its Opinion on the definition of consent, "considering the importance that some social networks have acquired, some categories of users (such as teenagers) will accept the receipt of behavioural advertising in order to avoid the risk of being partially excluded from social interactions. The user should be put

1021 General Data Protection Regulation, Art. 4 and Art. 7; Modernised Convention 108, Art. 5.

> in a position to give free and specific consent to receiving behavioural advertising, independently of his access to the social network service."[1022]

Under the General Data Protection Regulation, the personal data of children under the age of 16 cannot, in principle, be processed based on their consent.[1023] If consent for the processing is necessary, it must be given by the child's parent or guardian. Children merit specific protection due to the fact that they may be less aware of the risks and consequences involved in the data processing. This is very important in the context of social media, as children are more vulnerable to some of the negative effects the use of such media may entail, such as cyber-bulling, online stalking or identify theft.

Security and privacy/data protection by design and by default

The processing of personal data inherently entails security risks, given the constant possibility of a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised access or disclosure of the personal data processed. Under European data protection law, controllers and processors are required to implement appropriate technical and organisational measures to prevent any unauthorised interference with data processing operations. Social networking services providers falling within the scope of European data protection rules must also comply with this obligation.

The principles of privacy/data protection by design and by default require controllers to maintain security in the design of their products and to automatically apply suitable privacy and data protection settings. This means that when a person decides to joins a social network, the service provider may not automatically make all the information about the new service user available to all of its users. When joining the service, the default privacy and data protection settings should be such that information is only available to the individual's chosen contacts. Extending access to people beyond that list should only be possible after the user has taken action to manually change the default privacy and data protection settings. This may also have an impact in cases where a data breach occurs despite the security measures

1022 Article 29 Working Party (2011), *Opinion 15/2011 on the definition of consent*, WP 187, 13 July 2011, p. 18.

1023 See General Data Protection Regulation, Art. 8. EU Member States may provide by law for a lower age, provided that this is not below 13 years.

put in place. In such cases, service providers must notify the users affected where it is likely to result in a high risk to the rights and freedoms of the data subject.[1024]

Privacy/data protection by design and by default are particularly important in the context of SNS, as, in addition to the risks of unauthorised access involved in most types of processing, sharing personal information in social media poses additional security risks. These are often due to individuals' lack of understanding as to *who* may access their information, and how these people may use it. With the widespread use of social media, the number of identity theft incidents and victims has increased.

Example: Identity theft is a phenomenon whereby a person obtains information, data or documents belonging to another person (the victim), and then uses this information to impersonate the victim to obtain goods and services in the victim's name. Take Paul, for example, who has an account on a social media website. Paul is a teacher and an active member of his community, very outgoing and not particularly worried about the privacy and data protection settings of his social media account. He has a big list of contacts, sometimes including people he does not necessarily know personally. As he works in a big school, and has been quite popular coaching the school's football team, he thinks that these people are most likely parents or friends of the school. Paul's email address and birthday are displayed in his social media account. In addition, Paul regularly posts photos of his dog Toby, accompanied by lines such as "Me and Toby on our morning run". Paul has not realised that one of the most popular security questions to protect his email or mobile phone account is "what is the name of your pet". Using the information available on Paul's social media profile, Nick easily manages to hack Paul's accounts.

Rights of individuals

SNS providers must respect the rights of individuals (see Section 6.1), including the right to be informed about the purpose of processing and how personal data may be used for direct marketing purposes. Individuals must also be given the right to access the personal data they have generated in the social networking platform and request their deletion. Even where persons have consented to the processing

1024 *Ibid.*, Art. 34.

of personal data and uploaded information online, they should be able to ask to "be forgotten" if they no longer want to receive the social network's services. The right to data portability further enables users to receive a copy of the personal data they provided to the social networking services provider in a structured, commonly used and machine-readable format and to transfer their data from one social networking services provider to another.[1025]

Controllers

A difficult question that often arises in the context of social media is the question of who the controller is, meaning: who is the person with the obligation and responsibility to comply with the data protection rules. Social networking service providers are considered controllers under European data protection law. This is evident given the broad definition of "controller" and the fact that these service providers determine the purpose and means for the processing of the personal data shared by individuals. Under EU law, if they offer services to data subjects in the EU, controllers are required to comply with the provisions of the General Data Protection Regulation, even if they are not established in the EU.

Can users of social networking services also be regarded as controllers, however? Where individuals process personal data "in the course of a purely personal or household activity", data protection rules do not apply. This is known in European data protection law as the "household exemption". However, in some cases, a user of a social networking service may not be covered by the household exemption.

Users voluntarily share their personal information online. However, information shared online often includes personal information of other individuals.

Example: Paul has an account on a very popular social networking platform. Paul is trying to become an actor and uses his account to post photos, videos and posts explaining his passion for art. Popularity is important for his future; he has thus decided that his profile should not only be available to his close list of contacts but to all internet users, whether they are members of the network or not. Can Paul post photos and videos of him with his friend Sarah without her consent? As a primary school teacher, Sarah tries to keep her private life away from her employer, her students and their parents. Imagine

1025 General Data Protection Regulation, Art. 21.

a case where Sarah, who does not use social networks, finds out from their common friend Nick that a photo of her at a party with Paul was posted online. In such a case, Paul's data processing will not fall under EU law as it is covered by the "household exemption".

However, it remains crucial for users to be aware and mindful that uploading information about other individuals without their consent may infringe upon these individuals' privacy and data protection rights. Even where the household exemption applies – for example, if a user has a profile that is only made public to a list of contacts selected by him or her – the publication of personal information about others might still make the user liable. Although data protection rules do not apply if the household exemption does, liability might arise from the application of other national rules, such as defamation or violation of personality. Finally, only users of SNS are protected by the household exemptions: controllers and processors that provide the means for such private processing fall under EU data protection law.[1026]

With the reform of the Directive on privacy and electronic communications, the data protection, privacy and security rules that are applicable to telecommunication services providers under the current legal framework will also apply to machine-to-machine communications and electronic communications services, including, for instance, over the top services.

1026 *Ibid*., Recital 18.

Further reading

Chapter 1

Araceli Mangas, M. (ed.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Vienna, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C. 'Four fundamental rights: finding the balance', *International Data Privacy Law*, Vol. 6, No. 3, pp. 195–209.

González Fuster, G. and Gellert, G. (2012), 'The fundamental right of data protection in the European Union: in search of an uncharted right', *International Review of Law, Computers and Technology*, Vol. 26 (1), pp. 73–82.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwange, C. and Nouwt, S. (Eds.) (2009), *Reinventing Data Protection*, Springer.

Hijmans, H. (2016), *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU*, Springer.

Hustinx, P. (2016), 'EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation'.

Kranenborg, H. (2015), 'Google and the Right to be Forgotten', *European Data Protection Law Review*, Vol. 1, No. 1, pp. 70–79.

Lynskey, O. (2014), 'Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order', *International and Comparative Law Quarterly*, Vol. 63, No. 3, pp. 569–597.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press.

Kokott, J. and Sobotta, C. (2013), 'The distinction between privacy and data protection in the case law of the CJEU and the ECtHR', *International Data Privacy Law*, Vol. 3, No. 4, pp. 222–228.

EDRi, *An introduction to data protection*, Brussels.

Frowein, J. and Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C. and Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Munich, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. and Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, Munich, C. H. Beck.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. and Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerp, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. and Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Brussels, Emile Bruylant.

Simitis, S. (1997), 'Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?', *Neue Juristische Wochenschrift*, No. 5, pp. 281–288.

Warren, S. and Brandeis, L. (1890), 'The right to privacy', *Harvard Law Review,* Vol. 4, No. 5, pp. 193–220.

White, R. and Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Chapter 2

Acquisty, A., and Gross R. (2009), 'Predicting Social Security numbers from public data', *Proceedings of the National Academy of Science*, 7 July 2009.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., and Blondel V. D. (2013), 'Unique in the Crowd: the Privacy Bounds of Human Mobility', *Nature Scientific Reports*, Vol. 3, 2013.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

González Fuster, G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right in the EU*, Springer.

Morgan, R. and Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell.

Ohm, P. (2010), 'Broken promises of privacy: Responding to the surprising failure of anonymization', *UCLA Law Review*, Vol. 57, No. 6, pp. 1701–1777.

Samarati, P. and Sweeney, L. (1998), 'Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression', Technical Report SRI-CSL-98-04.

Sweeney, L. (2002), 'K-Anonymity: A Model for Protecting Privacy' *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, Vol. 10, No. 5, pp. 557–570.

Tinnefeld, M., Buchner, B. and Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Munich, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice.*

Chapters 3 to 6

Brühann, U. (2012), 'Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr' in: Grabitz, E., Hilf, M. and Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Munich, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrucken, Éditions universitaires européennes.

Curren, L. and Kaye, J. (2010), 'Revoking consent: a 'blind spot' in data protection law?', *Computer Law & Security Review*, Vol. 26, No. 3 pp. 273–283.

Dammann, U. and Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. and Papakonstantinou, V. (2012), 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis', *Computers & Law Magazine of SCL*, Vol. 22, No. 6, pp. 1–5.

De Hert, P. and Papakonstantinou, V. (2012), 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', *Computer Law & Security Review*, Vol. 28, No. 2, pp. 130–142.

Feretti, Federico (2012), 'A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after

the Lisbon treaty: Taking rights seriously', *European Review of Private Law*, Vol. 20, No. 2, pp. 473–506.

FRA (European Union Agency for Fundamental Rights) (2010), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxembourg, Publications Office of the European Union (Publications Office).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Conference edition), Vienna, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxembourg, Publications Office.

Irish Health Information and Quality Authority (2010), Guidance on Privacy Impact Assessment in Health and Social Care.

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I. and Saxby, S. (2011), '30 years on – The review of the Council of Europe Data Protection Convention 108', *Computer Law & Security Review*, Vol. 27, No. 3, pp. 223–231.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*.

Chapter 7

European Data Protection Supervisor (2014), Position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies.

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. and Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

Article 29 Working Party (2005), *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*.

Chapter 8

Blasi Casagran, C. (2016) *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, London, Routledge.

Boehm, F. (2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level,* Berlin, Springer.

Europol (2012), *Data Protection at Europol*, Luxembourg, Publications Office.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, The Hague, Eurojust.

De Hert, P. and Papakonstantinou, V. (2012), 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis', *Computers & Law Magazine of SCL*, Vol. 22, No. 6, pp. 1–5.

Drewer, D. and Ellermann, J. (2012), 'Europol's data protection framework as an asset in the fight against cybercrime', *ERA Forum*, Vol. 13, No. 3, pp. 381–395.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berlin, Springer.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), 'Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem', *European Law Review*, Vol. 36, No. 5, pp. 722–776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of External Relations, CLEER Working Papers 2013/2.

Chapter 9

Büllesbach, A., Gijrath, S., Poullet, Y. and Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. and Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), 'Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem', *European Law Review*, Vol. 36, No. 5, pp. 722–776.

Rosemary, J. and Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

Chapter 10

El Emam, K. and Álvarez, C. (2015), 'A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques', *International Data Privacy Law*, Vol. 5, No. 1, pp. 73–87.

Mayer-Schönberger, V. and Cate, F. (2013), 'Notice and consent in a world of Big Data', *International Data Privacy Law*, Vol. 3, No. 2, pp. 67–73.

Rubistein, I. (2013), 'Big Data: The End of Privacy or a New Beginning?', *International Data Privacy Law*, Vol. 3, No. 2, pp. 74–87.

Case law

Selected case law of the European Court of Human Rights

Access to personal data

Gaskin v. the United Kingdom, No. 10454/83, 7 July 1989
Godelli v. Italy, No. 33783/09, 25 September 2012
K.H. and Others v. Slovakia, No. 32881/04, 28 April 2009
Leander v. Sweden, No. 9248/81, 26 March 1987
M.K. v. France, No. 19522/09, 18 April 2013
Odièvre v. France [GC], No. 42326/98, 13 February 2003

Balancing data protection with freedom of expression and the right to information

Axel Springer AG v. Germany [GC], No. 39954/08, 7 February 2012
Bohlen v. Germany, No. 53495/09, 19 February 2015
Coudec and Hachette Filipacchi Associés v. France [GC], No. 40454/07, 10 November 2015
Magyar Helsinki Bizottság v. Hungary [GC], No. 18030/11, 8 November 2016
Müller and Others v. Switzerland, No. 10737/84, 24 May 1988
Vereinigung bildender Künstler v. Austria, No. 68345/01, 25 January 2007
Von Hannover v. Germany (No. 2) [GC], Nos. 40660/08 and 60641/08, 7 February 2012
Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, No. 931/13, 27 June 2017

Balancing data protection with freedom of religion

Sinan Işık v. Turkey, No. 21924/05, 2 February 2010

Challenges in online data protection

K.U. v. Finland, No. 2872/02, 2 December 2008

Consent of the data subject

Elberte v. Latvia, No. 61243/08, 13 January 2015
Sinan Işık v. Turkey, No. 21924/05, 2 February 2010
Y v. Turkey, No. 648/10, 17 February 2015

Correspondence

Amann v. Switzerland [GC], No. 27798/95, 16 February 2000
Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, No. 62540/00, 28 June 2007
Bernh Larsen Holding AS and Others v. Norway, No. 24117/08, 14 March 2013
Cemalettin Canli v. Turkey, No. 22427/04, 18 November 2008
D.L. v. Bulgaria, No. 7472/14, 19 May 2016
Dalea v. France, No. 964/07, 2 February 2010
Gaskin v. the United Kingdom, No. 10454/83, 7 July 1989
Haralambie v. Romania, No. 21737/03, 27 October 2009
Khelili v. Switzerland, No. 16188/07, 18 October 2011
Leander v. Sweden, No. 9248/81, 26 March 1987
Malone v. the United Kingdom, No. 8691/79, 2 August 1984
Rotaru v. Romania [GC], No. 28341/95, 4 May 2000
S. and Marper v. the United Kingdom [GC], Nos. 30562/04 and 30566/04, 4 December 2008
Shimovolos v. Russia, No. 30194/09, 21 June 2011
Silver and Others v. the United Kingdom, Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 March 1983
The Sunday Times v. the United Kingdom, No. 6538/74, 26 April 1979

Criminal record databases

Aycaguer v. France, No. 8806/12, 22 June 2017
B.B. v. France, No. 5335/06, 17 December 2009
Brunet v. France, No. 21010/10, 18 September 2014

M.K. v. France, No. 19522/09, 18 April 2013
M.M. v. the United Kingdom, No. 24029/07, 13 November 2012

Data security

Haralambie v. Romania, No. 21737/03, 27 October 2009
K.H. and Others v. Slovakia, No. 32881/04, 28 April 2009

DNA databases

S. and Marper v. the United Kingdom [GC], Nos. 30562/04 and 30566/04, 4 December 2008

GPS data

Uzun v. Germany, No. 35623/05, 2 September 2010

Health data

Avilkina and Others v. Russia, No. 1585/09, 6 June 2013
Biriuk v. Lithuania, No. 23373/03, 25 November 2008
I v. Finland, No. 20511/03, 17 July 2008
L.H. v. Latvia, No. 52019/07, 29 April 2014
L.L. v. France, No. 7508/02, 10 October 2006
M.S. v. Sweden, No. 20837/92, 27 August 1997
Szuluk v. the United Kingdom, No. 36936/05, 2 June 2009
Y v. Turkey, No. 648/10, 17 February 2015
Z v. Finland, No. 22009/93, 25 February 1997

Identity

Ciubotaru v. Moldova, No. 27138/04, 27 April 2010
Godelli v. Italy, No. 33783/09, 25 September 2012
Odièvre v. France [GC], No. 42326/98, 13 February 2003

Information concerning professional activities

G.S.B. v. Switzerland, No. 28601/11, 22 December 2015
M.N. and Others v. San Marino, No. 28005/12, 7 July 2015
Michaud v. France, No. 12323/11, 6 December 2012
Niemietz v. Germany, No. 13710/88, 16 December 1992

Interception of communication

Amann v. Switzerland [GC], No. 27798/95, 16 February 2000
Brito Ferrinho Bexiga Villa-Nova v. Portugal, No. 69436/10, 1 December 2015
Copland v. the United Kingdom, No. 62617/00, 3 April 2007
Halford v. the United Kingdom, No. 20605/92, 25 June 1997
Iordachi and Others v. Moldova, No. 25198/02, 10 February 2009
Kopp v. Switzerland, No. 23224/94, 25 March 1998
Liberty and Others v. the United Kingdom, No. 58243/00, 1 July 2008
Malone v. the United Kingdom, No. 8691/79, 2 August 1984
Mustafa Sezgin Tanrıkulu v. Turkey, No. 27473/06, 18 July 2017
Pruteanu v. Romania, No. 30181/05, 3 February 2015
Szuluk v. the United Kingdom, No. 36936/05, 2 June 2009

Obligations for duty bearers

B.B. v. France, No. 5335/06, 17 December 2009
I v. Finland, No. 20511/03, 17 July 2008
Mosley v. the United Kingdom, No. 48009/08, 10 May 2011

Personal data

Amann v. Switzerland [GC], No. 27798/95, 16 February 2000
Uzun v. Germany, No. 35623/05, 2010
Bernh Larsen Holding AS and Others v. Norway, No. 24117/08, 14 March 2013

Photos

Sciacca v. Italy, No. 50774/99, 11 January 2005
Von Hannover v. Germany, No. 59320/00, 24 June 2004

Right to be forgotten

Segerstedt-Wiberg and Others v. Sweden, No. 62332/00, 6 June 2006
Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, No. 931/13, 27 June 2017

Right to object

Leander v. Sweden, No. 9248/81, 26 March 1987
M.S. v. Sweden, No. 20837/92, 27 August 1997
Mosley v. the United Kingdom, No. 48009/08, 10 May 2011

Rotaru v. Romania [GC], No. 28341/95, 4 May 2000
Sinan Işık v. Turkey, No. 21924/05, 2 February 2010

Sensitive categories of data

Brunet v. France, No. 21010/10, 18 September 2014
I v. Finland, No. 20511/03, 17 July 2008
Michaud v. France, No. 12323/11, 6 December 2012
S. and Marper v. the United Kingdom [GC], Nos. 30562/04 and 30566/04, 4 December 2008

Supervision and enforcement (role of different actors, including supervisory authorities)

I v. Finland, No. 20511/03, 17 July 2008
K.U. v. Finland, No. 2872/02, 2 December 2008
Von Hannover v. Germany, No. 59320/00, 24 June 2004
Von Hannover v. Germany *(No. 2)* [GC], Nos. 40660/08 and 60641/08, 7 February 2012

Surveillance methods

Allan v. the United Kingdom, No. 48539/99, 5 November 2002
Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, No. 62540/00, 28 June 2007
Bărbulescu v. Romania [GC], No. 61496/08, 5 September 2017
D.L. v. Bulgaria, No. 7472/14, 19 May 2016
Dragojević v. Croatia, No. 68955/11, 15 January 2015
Karabeyoğlu v. Turkey, No. 30083/10, 7 June 2016
Klass and Others v. Germany, No. 5029/71, 6 September 1978
Rotaru v. Romania [GC], No. 28341/95, 4 May 2000
Szabó and Vissy v. Hungary, No. 37138/14, 12 January 2016
Taylor-Sabori v. the United Kingdom, No. 47114/99, 22 October 2002
Uzun v. Germany, No. 35623/05, 2 September 2010
Versini-Campinchi and Crasnianski v. France, No. 49176/11, 16 June 2016
Vetter v. France, No. 59842/00, 31 May 2005
Vukota-Bojić v. Switzerland, No. 61838/10, 18 October 2016
Roman Zakharov v. Russia [GC], No. 47143/06, 4 December 2015

Video surveillance

Köpke v. Germany, No. 420/07, 5 October 2010
Peck v. the United Kingdom, No. 44647/98, 28 January 2003

Voice samples

Wisse v. France, No. 71611/01, 20 December 2005
P.G. and J.H. v. the United Kingdom, No. 44787/98, 25 September 2001

Selected case law of the Court of Justice of the European Union

Case law related to the Data Protection Directive

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme'*, 4 May 2017
[Lawful processing principle: legitimate interest pursued by a third party]

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 9 March 2017
[Right to erasure of personal data; right to object to processing]

Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson* and *Others* [GC], 21 December 2016
[Confidentiality of electronic communications; providers of electronic communications services; obligation relating to the general and indiscriminate retention of traffic and location data; no prior review by a court or independent administrative authority; Charter of Fundamental Rights of the European Union; compatibility with EU law]

C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, 19 October 2016
[Definition of 'personal data'; Internet protocol addresses; storage of data by an online media services provider; national legislation not permitting the legitimate interest pursued by the controller to be taken into account]

C-362/14, *Maximilian Schrems v. Data Protection Commissioner* [GC], 6 October 2015
[Lawful processing principle; fundamental rights; invalidity of the Safe Harbour Decision; powers of the independent supervisory authorities]

C-230/14, *Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 October 2015
[Powers of national supervisory authorities]

C-201/14, *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others*, 1 October 2015
[Right to be informed about processing of personal data]

C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, 11 December 2014
[Concept of "data processing" and "controller"]

C-473/12, *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert and Others*, 7 November 2013
[Right to be informed about processing of personal data]

T-462/12 R, *Pilkington Group Ltd v. European Commission*, Order of the President of the General Court, 11 March 2013

C-342/12, *Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT)*, 30 May 2013
[Concept of 'personal data'; record of working time; principles relating to data quality and criteria for making data processing legitimate; access by the national authority responsible for monitoring working conditions; employer's obligation to make available the record of working time so as to allow its immediate consultation]

Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [GC], 8 April 2014
[Violation of EU primary law by the Data Retention Directive; lawful processing; purpose and storage limitation]

C-288/12, *European Commission v. Hungary* [GC], 8 April 2014
[Legitimacy of removal of office of the national data protection supervisor]

Joined cases C-141/12 and C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel* and *Minister voor Immigratie, Integratie en Asiel v. M and S*, 17 July 2014
[Scope of the right of access of a data subject; protection of individuals with regard to the processing of personal data; concept of 'personal data'; data relating to the applicant for a residence permit and legal analysis contained in an administrative document preparatory to the decision; Charter of Fundamental Rights of the European Union]

C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13 May 2014
[Obligations of search engine providers to refrain, on request of the data subject, from showing personal data in the search results; applicability of the Data Protection Directive; concept of "data processing"; meaning of "controllers"; balancing data protection with freedom of expression; the right to be forgotten]

C-614/10, *European Commission v. Republic of Austria* [GC], 16 October 2012
[Independence of a national supervisory authority]

Joined cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 November 2011
[Correct implementation of Article 7 (f) of the Data Protection Directive – "legitimate interests of others" – in national law]

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, 16 February 2012
[Obligation of social network providers to prevent unlawful use of musical and audio-visual works by network users]

C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 November 2011
[Information society; copyright; internet; 'peer-to-peer' software; Internet service providers; installation of a system for filtering electronic communications to prevent file sharing which infringes copyright; no general obligation to monitor information transmitted]

C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, 5 May 2011
[Necessity of renewed consent]

Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [GC], 9 November 2010
[Concept of "personal data"; proportionality of the legal obligation to publish personal data about the beneficiaries of certain EU agricultural funds]

C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*, 7 May 2009
[Right of access of the data subject]

C-518/07, *European Commission v. Federal Republic of Germany* [GC], 9 March 2010
[Independence of a national supervisory authority]

C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [GC], 16 December 2008
[Concept of 'journalistic activities' within the meaning of Article 9 Data Protection Directive]

C-524/06, *Heinz Huber v. Bundesrepublik Deutschland* [GC], 16 December 2008
[Legitimacy of holding data on foreigners in a statistical register]

C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [GC], 29 January 2008
[Concept of "personal data"; obligation of internet access providers to disclose identity of users of KaZaA file exchange programmes to intellectual property protection association]

C-101/01, *Criminal proceedings against Bodil Lindqvist*, 6 November 2003
[Special categories of personal data]

Joined cases C-465/00, C-138/01 and C-139/01, *Rechnungshof v. Österreichischer Rundfunk and Others* and *Christa Neukomm and Jospeh Lauermann v. Österreichischer Rundfunk*, 20 May 2003
[Proportionality of legal obligation to publish personal data about salaries of employees of certain categories of public sector related institutions]

C434/16, *Peter Nowak v. Data Protection Commissioner, Opinion of the Advocate General Kokott*, 20 July 2017
[Concept of personal data; access to one's own examination script; examiner's corrections]

C-291/12, *Michael Schwarz v. Stadt Bochum*, 17 October 2013
[Reference for a preliminary ruling; area of freedom, security and justice; biometric passport; fingerprints; legal basis; proportionality]

Case law related to Directive 2016/681

Opinion 1/15 of the Court (Grand Chamber), 26 July 2017
[Legal basis; draft agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data; compatibility of the draft agreement with Article 16 TFEU and Articles 7 and 8 and Article 52 (1) of the Charter of Fundamental Rights of the European Union]

Case law related to the EU Institutions Data Protection Regulation

C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (EFSA), European Commission,* 16 July 2015
[Access to documents]

C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd.* [GC], 29 June 2010
[Access to documents]

Case law related to Directive 2002/58/EC

C-536/15, *Tele2 (Netherlands) BV and Others v. Autoriteit Consument en Markt (AMC)*, 15 March 2017
[Principle of non-discrimination; making available personal data concerning subscribers for the purposes of the provision of publicly available directory enquiry services and directories; subscriber's consent; distinction on the basis of the Member State in which publicly available directory enquiry services and directories are provided]

Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestryrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others* [GC], 21 December 2016
[Confidentiality of electronic communications; providers of electronic communications services; obligation relating to the general and indiscriminate retention of traffic and location data; no prior review by a court or independent administrative authority; Charter of Fundamental Rights of the European Union; compatibility with EU law]

C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 November 2011
[Information society; copyright; internet; 'peer-to-peer' software; internet service providers; installation of a system for filtering electronic communications to prevent file sharing which infringes copyright; no general obligation to monitor information transmitted]

C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v. Perfect Communication Sweden AB*, 19 April 2012
[Copyright and related rights; processing of data by internet; infringement of an exclusive right; audio books made available via an FTP server via internet by an IP address supplied by an internet service provider; injunction issued against the internet service provider ordering it to provide the name and address of the user of the IP address]

Index

Case law of the Court of Justice of the European Union

Case law of the European Court of Human Rights

Case law of national courts

A great deal of information on the European Union Agency for Fundamental Rights is available on the internet. It can be accessed through the FRA website at fra.europa.eu.

Further information on the case law of the European Court of Human Rights is available on the Court's website: echr.coe.int. The HUDOC search portal provides access to judgments and decisions in English and/or French, translations into additional languages, legal summaries, press releases and other information on the work of the Court.

How to obtain Council of Europe publications

Council of Europe Publishing produces works in all the Organisation's spheres of reference, including human rights, legal science, health, ethics, social affairs, the environment, education, culture, sport, youth and architectural heritage. Books and electronic publications from the extensive catalogue may be ordered online: http://book.coe.int/.

A virtual reading room enables users to consult excerpts from the main works just published or the full texts of certain official documents at no cost.

Information on, as well as the full text of, the Council of Europe Conventions is available from the Treaty Office website: http://conventions.coe.int/.

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:
– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
– at the following standard number: +32 22999696 or
– by email via: https://europa.eu/european-union/contact_en

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, both for commercial and non-commercial purposes.

doi: 10.2811/343461 TK-05-17-225-EN-N

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

The rapid development of information technology has exacerbated the need for robust personal data protection, the right to which is safeguarded by both European Union (EU) and Council of Europe (CoE) instruments. Safeguarding this important right entails new and significant challenges as technological advances expand the frontiers of areas such as surveillance, communication interception and data storage. This handbook is designed to familiarise legal practitioners not specialised in data protection with this emerging area of the law. It provides an overview of the EU's and the CoE's applicable legal frameworks. It also explains key case law, summarising major rulings of both the Court of Justice of the European Union and the European Court of Human Rights. In addition, it presents hypothetical scenarios that serve as practical illustrations of the diverse issues encountered in this ever-evolving field.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS
Schwarzenbergplatz 11 - 1040 Vienna - Austria
Tel. +43 (1) 580 30-60 - Fax +43 (1) 580 30-699
fra.europa.eu – info@fra.europa.eu – @EURightsAgency

EUROPEAN COURT OF HUMAN RIGHTS
COUNCIL OF EUROPE
67075 Strasbourg Cedex - France
Tel. +33 (0) 3 88 41 20 18 - Fax +33 (0) 3 88 41 27 30
echr.coe.int - publishing@echr.coe.int – @ECHRPublication

EUROPEAN DATA PROTECTION SUPERVISOR
Rue Wiertz 60 – 1047 Brussels – Belgium
Tel. +32 2 283 19 00
www.edps.europa.eu – edps@edps.europa.eu – logo@EU_EDPS

Publications Office
ISBN 978-92-871-9849-5 (CoE)
ISBN 978-92-9491-901-4 (FRA)