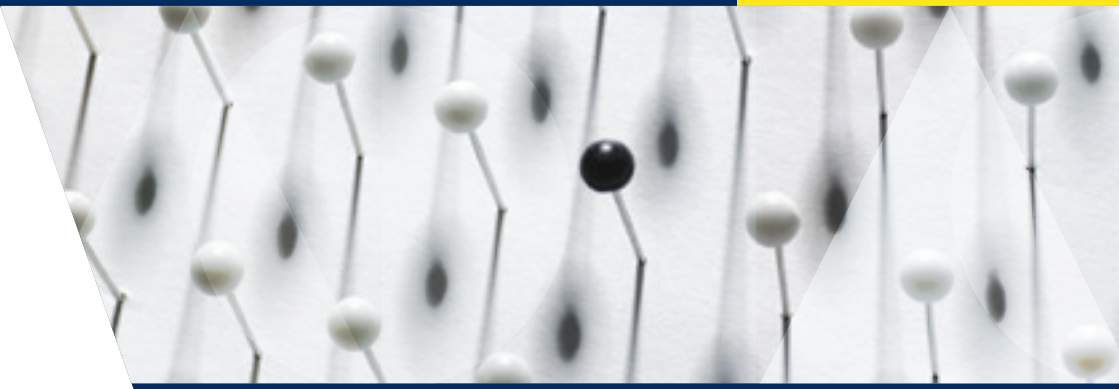
HANDBOOK



Handbook on European data protection law

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

The manuscript for this Handbook was completed in April 2014.
Updates will become available in future on the FRA website at: fra.europa.eu, the Council of Europe website at coe.int/dataprotection, and on the European Court of Human Rights website under the Case-Law menu at: echr.coe.int.

Europe Direct is a service to help you find answers to your questions about the European Union

Freephone number (*):

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Photo credit (cover & inside): © iStockphoto

More information on the European Union is available on the Internet (http://europa.eu).

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2014

ISBN 978-92-871-9934-8 (CoE)
ISBN 978-92-9239-461-5 (FRA)
doi:10.2811/69915

Printed in Belgium

Printed on process chlorine-free recycled paper (PCF)

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

Handbook on European data protection law

Foreword

This handbook on European data protection law is jointly prepared by the European Union Agency for Fundamental Rights (FRA) and the Council of Europe together with the Registry of the European Court of Human Rights. It is the third in a series of legal handbooks jointly prepared by FRA and the Council of Europe. In March 2011, a first handbook was published on European non-discrimination law and, in June 2013, a second one on European law relating to asylum, borders and immigration.

We have decided to continue our cooperation on a highly topical subject which affects all of us every day, namely the protection of personal data. Europe enjoys one of the most protective systems in this sphere, which is based on Council of Europe Convention 108, European Union (EU) instruments, as well as the case law of the European Court of Human Rights (ECtHR) and of the Court of Justice of the European Union (CJEU).

The aim of this handbook is to raise awareness and improve knowledge of data protection rules in European Union and Council of Europe member states by serving as the main point of reference to which readers can turn. It is designed for non-specialist legal professionals, judges, national data protection authorities and other persons working in the field of data protection.

With the entry into force of the Treaty of Lisbon in December 2009, the Charter of Fundamental Rights of the EU became legally binding, and with this the right to the protection of personal data was elevated to the status of a separate fundamental right. A better understanding of Council of Europe Convention 108 and EU instruments, which paved the way for data protection in Europe, as well as of the CJEU and ECtHR case law, is crucial for the protection of this fundamental right.

We would like to thank the Ludwig Boltzmann Institute of Human Rights for its contribution in drafting this handbook. We would also like to express our gratitude to the European Data Protection Supervisor's office for its feedback during the drafting phase. We thank in particular the data protection unit of the European Commission during the preparation of this handbook.

Philippe Boillat

Director General of Human Rights and Rule of Law Council of Europe

Morten Kjaerum

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, it was called the 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)
CRM	Customer relations management
C-SIS	Central Schengen Information System
EAW	European Arrest Warrant
EC	European Community
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EFTA	European Free Trade Association
ENISA	European Network and Information Security Agency
ENU	Europol National Unit
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
GPS	Global positioning system
JSB	Joint Supervisory Body
NGO	Non-governmental organisation
N-SIS	National Schengen Information System
OECD	Organisation for Economic Co-operation and Development
PIN	Personal identification number
PNR	Passenger name record
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 provides an overview of the law applicable to data protection in relation to the European Union (EU) and the Council of Europe (CoE).

The handbook is designed to assist legal practitioners who are not specialised in the field of data protection; it is intended for lawyers, judges or other practitioners as well as those working for other bodies, including non-governmental organisations (NGOs), who may be confronted with legal questions relating to data protection.

It is a first point of reference on both EU law and the European Convention on Human Rights (ECHR) on data protection, and it explains how this field is regulated under EU law and under the 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 first presents a single table of the applicable legal provisions, including important selected case law under the two separate European legal systems. Then the relevant laws of these two European orders are presented one after the other as they may apply to each topic. This allows the reader to see where the two legal systems converge and where they differ.

The tables at the beginning of each chapter outline the topics dealt with in that chapter, naming the applicable legal provisions and other relevant material, such as jurisprudence. The order of the topics may differ slightly from the structure of the text within the chapter, if this is deemed favourable for the concise presentation of the chapter's content. The tables cover both CoE and EU law. This should help the users to find the key information relating to their situation, especially if they are subject only to CoE law.

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 EU Member States will need to use both sections, as these states are bound by both legal orders. For those who need more information on a particular issue, a list of references to more specialised material can be found in the 'Further reading' section of the handbook.

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

EU law is found in legislative measures that have been adopted, in relevant provisions of the treaties and in the Charter of Fundamental Rights of the European Union, as interpreted in the case law of the Court of Justice of the European Union (CJEU, otherwise referred to, before 2009, as the European Court of Justice (ECJ)).

The case law described or cited in this handbook provides examples of an important body of both ECtHR and CJEU case law. The guidelines at the end of this handbook are intended to assist the reader in searching for case law online.

In addition, the practical illustrations with hypothetical scenarios are provided in textboxes on a blue background, to further illustrate the application of European data protection rules in practice, particularly where no specific case law of the ECtHR or the CJEU exists on the topic. Other textboxes, presented on a grey background, provide examples taken from sources other than case law, such as legislation.

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 8 cover the following issues:

- data protection terminology;
- key principles of European data protection law;
- rules of European data protection law;
- data subjects' rights and their enforcement;
- transborder data flow;
- data protection in the context of police and criminal justice;
- other specific European data protection laws.

1

Context and background of European data protection law

EU	Issues covered	CoE
The right to data protection		
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		ECHR, Article 8 (right to respect for private and family life, home and correspondence) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)
Balancing rights		
CJEU, Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, 2010	In general	
CJEU, C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, 2008	Freedom of expression	ECtHR, *Axel Springer AG v. Germany*, 2012 ECtHR, *Mosley v. the United Kingdom*, 2011
	Freedom of arts and sciences	ECtHR, *Vereinigung bildender Künstler v. Austria*, 2007
CJEU, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 2008	Protection of property	
CJEU, C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd*, 2010	Access to documents	ECtHR, *Társaság a Szabadságjogokért v. Hungary*, 2009

1.1. The right to data protection

Key points

- Under Article 8 of the ECHR, a right to protection against the collection and use of personal data forms part of the right to respect for private and family life, home and correspondence.
- CoE Convention 108 is the first international legally binding instrument dealing explicitly with data protection.
- Under EU law, data protection was regulated for the first time by the Data Protection Directive.
- Under EU law, data protection has been acknowledged as a fundamental right.

A right to protection of an individual's private sphere against intrusion from others, especially from the state, was laid down in an international legal instrument for the first time in Article 12 of the United Nations (UN) Universal Declaration of Human Rights (UDHR) of 1948 on respect for private and family life.[1] The UDHR influenced the development of other human rights instruments in Europe.

1.1.1. 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 European Convention on Human Rights (ECHR) in 1950, which entered into force in 1953.

States 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 provisions of the Convention.

To ensure that the Contracting Parties observe their obligations under the ECHR, the European Court of Human Rights (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. In 2013, the Council of Europe comprised 47 member states, 28 of which are also EU Member States. An applicant

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

before the ECtHR does not need to be a national of one of the member states. The ECtHR can also examine inter-state cases brought by one or more CoE member states against another member state.

The right to protection of personal data 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.[2]

Throughout its jurisprudence the ECtHR has examined many situations in which the issue of data protection arose, not least those concerning interception of communication,[3] various forms of surveillance[4] and protection against storage of personal data by public authorities.[5] It has clarified that Article 8 of the ECHR not only obliged states to refrain from any actions which might violate this Convention right, but that they were in certain circumstances also under positive obligations to actively secure effective respect for private and family life.[6] Many of these cases will be referred to in detail in the appropriate chapters.

1.1.2. Council of Europe Convention 108

With of the emergence of information technology in the 1960s, a growing need developed 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 the protection of personal data, referring to Article 8 of the ECHR.[7] In 1981, a Convention for the protection of individuals with regard to the automatic processing of personal data (Convention 108)[8] was opened for

2 CoE, European Convention on Human Rights, CETS No. 005, 1950.

3 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.

4 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.

5 See, for example: ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987; ECtHR, *S. and Marper v. the United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008.

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

7 CoE, 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; CoE, 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.

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

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 sector, such as data processing by the judiciary and law enforcement authorities. It protects the individual against abuses, which may accompany the collection and processing of personal data, and seeks, at the same time, to regulate the transborder flow of personal data. As regards the collection and processing of personal data, the principles laid down in the convention concern, in particular, fair and lawful collection and automatic processing of data, stored for specified legitimate purposes and not for use for ends incompatible with these purposes nor kept for longer than is necessary. They also concern the quality of the data, in particular that they must be adequate, relevant and not excessive (proportionality) as well as accurate.

In addition to providing guarantees on the collection and processing of personal data, 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.

Although the convention provides for free flow of personal data between State Parties to the convention, it also imposes some restrictions on those flows to states where legal regulation does not provide equivalent protection.

In order to further develop the general principles and rules laid down in Convention 108, several recommendations that are not legally binding have been adopted by the Committee of Ministers of the CoE (see Chapters 7 and 8).

All EU Member States have ratified Convention 108. In 1999, Convention 108 was amended to enable the EU to become a Party.[9] In 2001, an Additional Protocol to Convention 108 was adopted, introducing provisions on transborder data flows

9 CoE, Amendments to the Convention for the protection of individuals with regard to automatic processing of Personal Data (ETS No. 108) allowing the European Communities to accede, adopted by the Committee of Ministers, in Strasbourg, on 15 June 1999; Art. 23 (2) of the Convention 108 in its amended form.

to non-parties, so-called third countries, and on the mandatory establishment of national data protection supervisory authorities. [10]

Outlook

Following a decision to modernise Convention108, a public consultation carried out in 2011 made it possible to confirm the two main objectives of that work: reinforcing the protection of privacy in the digital area and strengthening the convention's follow-up mechanism.

Convention 108 is open for accession to non-member states of the CoE, including non-European countries. The Convention's potential as a universal standard and its open character could serve as a basis for promoting data protection at global level.

So far, 45 of the 46 Contracting Parties to Convention 108 are member states of the CoE. Uruguay, the first non-European country, acceded in August 2013 and Morocco, which has been invited to accede to Convention 108 by the Committee of Ministers, is in the process of formalising accession.

1.1.3. European Union data protection law

EU law is composed of treaties 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 approved by all EU Member States and are also referred to as '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 are often referred to as 'secondary EU law'.

The principal EU legal instrument on data protection is 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*).[11] It was adopted in 1995, at a time when several Member States had already adopted national data protection laws. Free movement of goods, capital, services and people within the internal market required the

10 CoE, 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.

11 Data Protection Directive, OJ 1995 L 281, p. 31.

free flow of data, which could not be realised unless the Member States could rely on a uniform high level of data protection.

As the aim of adopting the Data Protection Directive was harmonisation[12] of data protection law at the national level, the directive affords a degree of specificity comparable to that of the (then) existing national data protection laws. For the CJEU, "Directive 95/46 is intended [...] to ensure that the level of protection of the rights and freedoms of individuals with regard to the processing of personal data is equivalent in all Member States. [...] The approximation of the national laws applicable in this area must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the EU. Accordingly, [...] the harmonisation of those national laws is not limited to minimal harmonisation but amounts to harmonisation which is generally complete."[13] Consequently, the EU Member States have only limited freedom to manoeuvre when implementing the directive.

The Data Protection Directive is designed to give substance to the principles of the right to privacy already contained in Convention 108, and to expand them. The fact that all 15 EU Member States in 1995 were also Contracting Parties to Convention 108 rules out the adoption of contradictory rules in these two legal instruments. The Data Protection Directive, however, draws on the possibility, provided for in Article 11 of Convention 108, of adding on instruments of protection. In particular, the introduction 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 taken over into CoE law in 2001 by the Additional Protocol to Convention 108.)

The territorial application of the Data Protection Directive extends beyond the 28 EU Member States, including also the non-EU Member States that are part of the European Economic Area (EEA)[14] – namely Iceland, Liechtenstein and Norway.

The CJEU in Luxembourg has jurisdiction to determine whether a Member State has fulfilled its obligations under the Data Protection Directive and to give preliminary rulings concerning the validity and interpretation of the directive, in order to ensure

12 See, for example, Data Protection Directive, Recitals 1, 4, 7 and 8.

13 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. 28-29.

14 Agreement on the European Economic Area, OJ 1994 L 1, which entered into force on 1 January 1994.

its effective and uniform application in the Member States. An important exemption from the applicability of the Data Protection Directive is the so-called household exemption, namely the processing of personal data by private individuals for merely personal or household purposes.[15] Such processing is generally seen as part of the freedoms of the private individual.

Corresponding to EU primary law in force at the time of the adoption of the Data Protection Directive, the material scope of the directive is limited to matters of the internal market. Outside its scope of application are, most importantly, matters of police and criminal justice cooperation. Data protection in these matters arises from different legal instruments, which are described in detail in Chapter 7.

As the Data Protection Directive could address only EU Member States, an additional legal instrument was needed in order to establish data protection for the processing of personal data by institutions and bodies of the EU. 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.[16]

Additionally, even in areas covered by the Data Protection Directive, more detailed data protection provisions are often needed in order to achieve the necessary clarity in balancing other legitimate interests. Two examples are the Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector (*Directive on privacy and electronic communications*)[17] and the Directive 2006/24/EC 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 (*Data Retention Directive*, invalidated on 8 April 2014).[18] Other examples will be discussed in Chapter 8. Such provisions must be in line with the Data Protection Directive.

15 Data Protection Directive, Art. 3 (2) second indent.

16 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.

17 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.

18 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, *(Data Retention Directive),* OJ 2006 L 105, invalidated on 8 April 2014.

The Charter of Fundamental Rights of the European Union

The original treaties of the European Communities did not contain any reference to human rights or their protection. As cases came before the then European Court of Justice (ECJ) alleging human rights violations in areas within the scope of EU law, however, it developed a new approach. 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 the 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). This Charter 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.

Although originally only a political document, the Charter became legally binding[19] as EU primary law (see Article 6 (1) of the TEU) with the coming into force of the Lisbon Treaty on 1 December 2009.[20]

EU primary law also contains a general EU competence to legislate on data protection matters (Article 16 of the TFEU).

The Charter not only guarantees the respect for private and family life (Article 7), but also establishes the right to data protection (Article 8), explicitly raising the level of this protection to that of a fundamental right in EU law. EU institutions as well as Member States must observe and guarantee this right, which also applies to 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

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

20 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.

Charter ensures that an independent authority will control the implementation of these principles.

Outlook

In January 2012, the European Commission proposed a data protection reform package, stating that the current rules on data protection needed to be modernised in light of rapid technological developments and globalisation. The reform package consists of a proposal for a General Data Protection Regulation,[21] meant to replace the Data Protection Directive, as well as a new General Data Protection Directive[22] which shall provide for data protection in the areas of police and judicial cooperation in criminal matters. At the time of the publication of this handbook, discussion on the reform package was ongoing.

1.2. Balancing rights

Key point

- The right to data protection is not an absolute right; it must be balanced against other rights.

The fundamental right to the protection of personal data under Article 8 of the Charter "is not, however, an absolute right, but must be considered in relation to its function in society".[23] Article 52 (1) of the Charter thus accepts 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 these limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are

21 European Commission (2012), *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012) 11 final, Brussels, 25 January 2012.

22 European Commission (2012), *Proposal for 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 the free movement of such data (General Data Protection Directive)*, COM(2012) 10 final, Brussels, 25 January 2012.

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

necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.[24]

In the ECHR system, data protection is guaranteed by Article 8 (right to respect for private and family life) and, as in the Charter system, this right needs to be applied while respecting the scope of other competing rights. Pursuant to Article 8 (2) of the ECHR, "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society [...] for the protection of the rights and freedoms of others".

Consequently, 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 ECHR and Article 8 of the Charter.[25] Several important examples will illustrate how this balance is reached.

1.2.1. Freedom of expression

One of the rights likely to come into conflict 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". Article 11 corresponds to Article 10 of the ECHR. Pursuant to Article 52 (3) of the Charter, insofar as it contains rights which 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 which 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 they must be necessary in a democratic society "for the

24 *Ibid.*, para. 50.

25 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*, 29 January 2008, para. 68. See also Council of Europe (2013), Case law of the European Court of Human Rights concerning the protection of personal data, DP (2013) Case law, available at: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP 2013 Case Law_Eng_FINAL.pdf.

protection [...] of the reputation or rights of others" . This concept covers the right to data protection.

The relationship between the protection of personal data and freedom of expression is governed by Article 9 of the Data Protection Directive, entitled 'Processing of personal data and freedom of expression'.[26] According to this article, Member States are required to provide for a number of derogations or limitations in relation to the protection of data and, therefore, in relation to the fundamental right to privacy, specified in Chapters II, IV and VI of the directive. Those derogations must be made solely for journalistic purposes or the purpose of artistic or literary expression, which fall within the scope of the fundamental right to freedom of expression, in so far as they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

Example: In *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*,[27] the CJEU was asked to interpret Article 9 of the Data Protection Directive and to define the relationship between data protection and the freedom of the press. The Court had to examine Markkinapörssi and Satamedia's dissemination of tax data on some 1.2 million natural persons lawfully obtained from the Finnish tax authorities. In particular, the Court had to verify whether the processing of personal data, which the tax authorities made available, in order 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 Satakunnan's activities were 'processing of personal data' within the meaning of Article 3 (1) of the Data Protection Directive, the Court went on to construe Article 9 of the directive. The Court 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, in order to achieve a balance between the two fundamental rights, the derogations and limitations of the right to data protection must apply only insofar as is strictly necessary. In those circumstances, the Court considered that activities such as those carried out by Markkinapörssi and Satamedia concerning data from documents which 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,

26 Data Protection Directive, Art. 9.

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

opinions or ideas, irrespective of the medium used to transmit them. The Court 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 in this particular case.

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*,[28] the ECtHR held that a ban imposed by a domestic court on the owner of a newspaper who wanted to publish an article on the arrest and conviction of a well-known actor violated Article 10 of the ECHR. The ECtHR reiterated criteria that it had established in its case law when balancing the right to freedom of expression against the right to respect for private life:

- first, whether the event that the published article concerned was of general interest: the arrest and conviction of a person was a public judicial fact and therefore of public interest;
- second, whether the person concerned was a public figure: the person concerned was an actor sufficiently well known to qualify as a public figure;
- third, how the information was obtained and whether it was reliable: the information had been provided by the public prosecutor's office and the accuracy of the information contained in both publications was not in dispute between the parties.

Therefore, the ECtHR ruled that 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: In *Von Hannover v. Germany (No. 2)*,[29] the ECtHR found no violation of the right to respect for private life under Article 8 of the ECHR, when Princess Caroline of Monaco was refused an injunction against the publication of a

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

29 ECtHR, *Von Hannover v. Germany (No. 2)* [GC], Nos. 40660/08 and 60641/08, 7 February 2012, paras. 118 and 124.

photograph of her and her husband taken during a skiing holiday. The photograph was accompanied by an article reporting on, among other issues, Prince Rainier's poor health. The ECtHR concluded that the domestic courts had carefully balanced the publishing companies' right to freedom of expression against the applicants' right to respect for their private life. The domestic courts' characterisation of Prince Rainier's illness as an event of contemporary society could not be considered unreasonable and the ECtHR was able to accept that the photograph, considered in light of the article, did at least to some degree contribute to a debate of general interest. The Court concluded that there had not been a violation of Article 8 of the ECHR.

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

Example: In *Mosley v. the United Kingdom*,[30] a national weekly newspaper published intimate photographs of the applicant. He then alleged a violation of Article 8 of the ECHR because he had been unable to seek an injunction before the publication of the photos in question due to the absence of any pre-notification requirement for the newspaper in case of publication of material capable of violating one's right to privacy. 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. Regarding the chilling effect to which a pre-notification requirement might give rise, to the doubts about its effectiveness and to 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 *Biriuk v. Lithuania*,[31] the applicant claimed damages from a daily newspaper because it had published an article reporting that she was HIV positive. That information had allegedly been confirmed by the medics at the local

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

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

hospital. The ECtHR did not deem the article in question to contribute to any debate of general interest and reiterated that the protection of personal data, not least medical data, was of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the ECHR. The Court attached particular significance to the fact that, according to the report in the newspaper, medical staff of a hospital had provided information about the applicant's HIV infection in evident breach of their obligation to medical secrecy. Consequently, the state had failed to secure the applicant's right to respect for her private life. The Court concluded that there had been a violation of Article 8.

1.2.2. Access to documents

Freedom of information according to Article 11 of the Charter and Article 10 of the ECHR protects the right not only to impart but also to *receive* information. There is a growing realisation of the importance of government transparency for the functioning of a democratic society. In the last 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*).[32] **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*).[33] Article 42 of the Charter and Article 15 (3) of the TFEU have extended this right of access "to documents of the institutions, bodies, offices and agencies of the Union, regardless of their form". In accordance with Article (52) 2 of the Charter, the right of access to documents is also exercised under the conditions and within the limits for which provision is made in Article 15 (3) of TFEU. This right may come into conflict with the right to data protection if access to a document would reveal others' personal data. Requests for access to documents or

32 Council of Europe, Committee of Ministers (2002), 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.

33 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.

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 *European Commission v. Bavarian Lager*,[34] the CJEU defined the scope of the protection of personal data in the context of access to documents of EU institutions and the relationship between Regulations Nos. 1049/2001 (*Access to Documents Regulation*) and 45/2001 (*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 decided to institute 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 which had been 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 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 Data Protection Regulation. Since it was not satisfied with this position, Bavarian Lager brought an action before the Court of First Instance, which annulled the Commission decision by judgment of 8 November 2007 (case T-194/04, *Bavarian Lager v. Commission*), considering in particular 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 constitute an undermining of private life and did not place the private lives of those persons in any danger.

On appeal by the Commission, the CJEU annulled the judgment of the Court of First Instance. 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

34 CJEU, C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd.*, 29 June 2010, paras. 60, 63, 76, 78 and 79.

thus seeks to obtain access to documents including personal data, the provisions of the 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 Data Protection Regulation.

According to this judgment, interference with the right to data protection with respect to access to documents needs a specific and justified reason. The right of access to documents cannot automatically overrule the right to data protection.[35]

A particular aspect of an access request was addressed in the following judgment of the ECtHR.

Example: In *Társaság a Szabadságjogokért v. Hungary*,[36] the applicant, a human rights NGO, had required from the Constitutional Court access to information about a pending case. Without consulting the member of parliament who had brought the case before it, the Constitutional Court refused the access request on the ground that complaints before it could be made available to outsiders only with the approval of the complainant. Domestic courts upheld this refusal, on the grounds that the protection of such personal data could not be overridden by other lawful interests, including the accessibility of public information. The applicant had acted as a 'social watchdog', whose activities warranted similar protection to those afforded the press. In relation to freedom of the press,

35 See, however, the detailed deliberations in European Data Protection Supervisor (EDPS) (2011), *Public access to documents containing personal data after the* Bavarian Lager *ruling*, Brussels, 24 March 2011, available at: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

36 ECtHR, *Társaság a Szabadságjogokért v. Hungary*, No. 37374/05, 14 April 2009; see paras. 27, 36–38.

the ECtHR had consistently held that the public had the right to receive information of general interest. The information sought by the applicant was "ready and available" and did not require any collection of data. In such circumstances, the state had an obligation not to impede the flow of information sought by the applicant. In sum, the ECtHR considered that obstacles designed to hinder access to information of public interest might discourage those working in the media or related fields from performing their vital role of a 'public watchdog'. The Court concluded that there had been a violation of Article 10.

Under EU law, the importance of transparency is firmly established. The principle of transparency is enshrined in Articles 1 and 10 of the TEU and in Article 15 (1) of the TFEU. [37] According to Recital 2 of the Regulation (EC) No. 1049/2001, it enables citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen in a democratic system.[38]

Following this reasoning, Council Regulation (EC) No. 1290/2005 on the financing of the common agricultural policy and Commission Regulation (EC) No. 259/2008 laying down detailed rules for its application require the publication of information on the beneficiaries of certain EU funds in the agricultural sector and the amounts received per beneficiary.[39] The publication should contribute to public control of the appropriate use of public funds by the administration. The proportionality of this publication was contested by several beneficiaries.

Example: In *Volker and Markus Schecke and Hartmut Eifert v. Land Hessen*,[40] 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.

37 EU (2012), Consolidated versions of the Treaty on European Union and of the TFEU, OJ 2012 C 326.

38 CJEU, C-41/00 P, *Interporc Im- und Export GmbH v. Commission of the European Communities*, 6 March 2003, para. 39; and CJEU, C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd.*, 29 June 2010, para. 54.

39 Council Regulation (EC) No. 1290/2005 of 21 June 2005 on the financing of the common agricultural policy, OJ 2005 L 209; and 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.

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

The Court, 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 Court considered 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, including 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) Charter. The Court thus declared partially invalid EU legislation on the publication of information relating to the beneficiaries of European agricultural funds.

1.2.3. Freedom of the arts and sciences

Another right to balance against the right to respect for private life and to data protection is the freedom of the arts and sciences, explicitly protected under Article 13 of the Charter. This right is deduced primarily from the right to freedom of thought and expression and it 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.[41] The right guaranteed by Article 13 of the Charter may also be subject to the limitations authorised by Article 10 of the ECHR.[42]

Example: In *Vereinigung bildender Künstler v. Austria*,[43] 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 accepting his request. The ECtHR reiterated that Article 10 of the ECHR was applicable to communicating ideas that offended, shocked or disturbed the state or any

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

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

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

section of the population. Those who created, performed, distributed or exhibited works of art contributed to the exchange of ideas and opinions and the state had 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.

In relation to science, European data protection law is aware of the special value of science to society. Therefore, the general restrictions for the use of personal data are diminished. The Data Protection Directive and Convention 108 both permit the retention of data for scientific research once they are no longer needed for the initial purpose of their collection. Furthermore, the subsequent use of personal data for scientific research shall not be considered an incompatible purpose. National law is charged with the task of developing more detailed provisions, including the necessary safeguards, to reconcile the interest in scientific research with the right to data protection (see also Sections 3.3.3 and 8.4) .

1.2.4. Protection of 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 Charter. One important aspect of the right to property is the protection of intellectual property, explicitly mentioned in Article 17 (2) of the Charter. Several directives can be found in the EU legal order, aiming at the effective protection of 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, against the right to data protection.[44] There have been cases where

44 ECtHR, *Ashby Donald and others v. France,* No. 36769/08, 10 January 2013.

copyright protection institutions demanded that internet 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*[45] 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 audiovisual 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, whom 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 in order 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 Court concluded that these three directives, as well as the Directive on privacy and electronic communications (2002/58/EC), do not preclude Member States from laying down an obligation to disclose personal data in the context of civil proceedings, to ensure the effective protection of copyright.

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.

The Court 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

45 CJEU, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 29 January 2008, paras. 54 and 60.

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."[46]

46 *Ibid.*, paras. 65 and 68; see also CJEU, C-360/10, *SABAM v. Netlog N.V.*, 16 February 2012.

2 Data protection terminology

EU	Issues covered	CoE
Personal data		
Data Protection Directive, Article 2 (a) CJEU, Joined cases C-92/09 and C-93/09, *Volker and Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen*, 9 November 2010 CJEU, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 29 January 2008	**Legal definition**	Convention 108, Article 2 (a) ECtHR, *Bernh Larsen Holding AS and Others v. Norway*, No. 24117/08, 14 March 2013
Data Protection Directive, Article 8 (1) CJEU, C-101/01, *Bodil Lindqvist*, 6 November 2003	**Special categories of personal data (sensitive data)**	Convention 108, Article 6
Data Protection Directive, Article 6 (1) (e)	**Anonymised and pseudonymised data**	Convention 108, Article 5 (e) Convention 108, Explanatory report, Article 42
Processing of data		
Data Protection Directive, Article 2 (b) CJEU, C-101/01, *Bodil Lindqvist*, 6 November 2003	**Definitions**	Convention 108, Article 2 (c)
Users of data		
Data Protection Directive, Article 2 (d)	**Controller**	Convention 108, Article 2 (d) Profiling Recommendation, Article 1 (g) *
Data Protection Directive, Article 2 (e) CJEU, C-101/01, *Bodil Lindqvist*, 6 November 2003	**Processor**	Profiling Recommendation Article 1 (h)

Data Protection Directive, Article 2 (g)	**Recipient**	Convention 108, Additional Protocol, Article 2 (1)
Data Protection Directive, Article 2 (f)	**Third party**	
Consent		
Data Protection Directive, Article 2 (h) CJEU, C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, 5 May 2011	**Definition and requirements for valid consent**	Medical Data Recommendation, Article 6, and various subsequent recommendations

Note: *Council of Europe, Committee of Ministers (2010), Recommendation Rec(2010)13 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 at least identifiable person, the data subject.
- A person is identifiable if additional information can be obtained without unreasonable effort, allowing the identification of the data subject.
- 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 Convention 108 and in the Data Protection Directive, which require enhanced protection and, therefore, are subject to a special legal regime.
- Data are anonymised if they no longer contain any identifiers; they are pseudonymised if the identifiers are encrypted.
- In contrast to anonymised data, pseudonymised data are personal data.

2.1.1. Main aspects of the concept of personal data

Under EU law as well as **under CoE law**, 'personal data' are defined as information relating to an identified or identifiable natural person,[47] that is, information about a person whose identity is either manifestly clear or can at least be established by obtaining additional information.

47 Data Protection Directive, Art. 2 (a); Convention 108, Art. 2 (a).

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

A person

The right to data protection developed out of the right to respect for private life. The concept of private life relates to human beings. Natural persons are, therefore, the primary beneficiaries of data protection. According to the Opinion of the Article 29 Working Party, furthermore, only a *living being* is protected under European data protection law.[48]

The ECtHR's jurisprudence concerning Article 8 of the ECHR shows that it may be difficult to completely separate matters of private and professional life.[49]

> Example: In *Amann v. Switzerland,*[50] authorities intercepted a business-related telephone call to the applicant. Based on that call, the authorities investigated the applicant and filled in a card on the applicant for the national security card index. Although the interception concerned a business-related telephone call, the ECtHR considered the storing of data about this call as relating to the private life of the applicant. It pointed out that the term 'private life' must not be interpreted restrictively, in particular, since respect for private life comprised the right to establish and develop relationships with other human beings. Furthermore, there was no reason of principle to justify excluding activities of a professional or business nature from the notion of 'private life'. Such a broad interpretation corresponded to that of Convention 108. The ECtHR further found that the interference in the applicant's case had not been in accordance with the law since domestic law did not contain specific and detailed provisions on the gathering, recording and storing of information. It thus concluded that there had been a violation of Article 8 of the ECHR.

Furthermore, if matters of professional life may also be the subject of data protection, it seems questionable that only natural persons should be afforded protection. Rights under the ECHR are guaranteed not only to natural persons but to everyone.

48 Article 29 Working Party (2007), *Opinion 4/2007 on the concept of personal data*, WP 136, 20 June 2007, p. 22.

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

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

There is jurisprudence of the ECtHR giving judgment on applications of legal persons alleging violation of their right to protection against the use of their data under Article 8 of the ECHR. The Court, however, examined the case under the right to respect for home and correspondence, rather than under private life:

> Example: *Bernh Larsen Holding AS and Others v. Norway*[51] concerned a complaint by three Norwegian companies about a tax authority decision ordering them to provide the tax auditors with a copy of all data on a computer server the three 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' for the purpose of 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 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 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 business companies and associations in their domestic law. **EU data protection law** does not, in general, cover the protection of legal persons with regard to the data processing that concerns them. The national regulators are free to regulate on that subject.[52]

> Example: In *Volker and Markus Schecke and Hartmut Eifert v. Land Hessen*,[53] 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

51 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.

52 Data Protection Directive, Recital 24.

53 CJEU, Joined cases C-92/09 and C-93/09, *Volker and Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen*, 9 November 2010, para. 53.

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 […]".[54]

Identifiability of a person

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

- an individual is identified in this information; or
- if an individual, while not identified, is described in 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. 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.[55]

The legal definitions of personal data do not further clarify when a person is considered to be identified.[56] Evidently identification 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. In exceptional cases, other identifiers can have a similar effect to a name. For instance, for public figures it may be enough to refer to the position of the person, such as President of the European Commission.

Example: In *Promusicae*,[57] 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

54 *Ibid.*, para. 52.

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

56 See also ECtHR, *Odièvre v. France* [GC], No. 42326/98, 13 February 2003; and ECtHR, *Godelli v. Italy*, No. 33783/09, 25 September 2012.

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

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 [...]. That communication of information which, as Promusicae submits and Telefónica does not contest, is stored by Telefónica constitutes the processing of personal data within the meaning of the first paragraph of Article 2 of Directive 2002/58, read in conjunction with Article 2 (b) of Directive 95/46".

As many names are not unique, establishing the identity of a person may need additional identifiers to ensure that a person is not confused with someone else. Date and place of birth are often used. In addition, personalised numbers have been introduced in some countries in order to better distinguish between citizens. Biometric data, such as fingerprints, digital photos or iris scans, are becoming increasingly important to identifying persons in the technological age.

For the applicability of European data protection law, however, there is no need for high-quality identification of the data subject; it is sufficient that the person concerned be identifiable. A person is considered identifiable if a piece of information contains elements of identification through which the person can be identified, directly or indirectly.[58] According to Recital 26 of the Data Protection Directive, 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 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 personal data. Licence plates, it says, are data about anonymous persons. 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 does not accord with Recital 26 of the Data Protection Directive. 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

58 Data Protection Directive, Art. 2 (a).

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 do 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.

Under CoE law, identifiability is understood in a similar way. Article 1 (2) of the Payment Data Recommendation,[59] for instance, states that a person shall not be regarded as 'identifiable' if identification requires an unreasonable amount of time, cost or manpower.

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 means of 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; 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, sometimes together with PINs, electronic signatures are an instrument especially capable of identifying and authenticating a person in electronic communications.

Nature of the data

Any kind of information can be personal data provided that it relates to a 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, even though it may just reflect, in part or whole, the superior's personal

59 CoE, Committee of Ministers (1990), Recommendation No. R Rec(90) 19 on the protection of personal data used for payment and other related operations, 13 September 1990.

opinion, such as: "the employee is not dedicated to his 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 as well as information about his or her professional or public life.

In the *Amann case*,[60] the ECtHR interpreted the term 'personal data' as not being limited to matters of the private sphere of an individual (see Section 2.1.1.). This meaning of the term 'personal data' is also relevant for the Data Protection Directive:

Example: In *Volker and Markus Schecke and Hartmut Eifert v. Land Hessen*,[61] 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 the Convention, 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".

Data relate to persons also if the content of the information indirectly reveals data about a person. In some cases, where there is a close link between an object or an event – e.g. a mobile phone, a car, an accident – on the one hand, and a person – e.g. as its owner, user, victim – on the other, information about an object or about an event ought also to be considered personal data.

Example: In *Uzun v. Germany,*[62] the applicant and another man were placed under surveillance via a global positioning system (GPS) device fitted in the other man's car because of their suspected involvement in bomb attacks. In this case, the ECtHR held that the applicant's observation via GPS amounted to interference in his private life as protected by Article 8 of the ECHR. However, the GPS surveillance had been in accordance with the law as well as proportionate to the legitimate aim of investigating several counts of attempted murder

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

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

62 ECtHR, *Uzun v. Germany*, No. 35623/05, 2 September 2010.

and was therefore necessary in a democratic society. The Court held that there had been no violation of Article 8 of the ECHR.

Form of appearance of the data

The form in which the personal data is stored or used is not relevant to the applicability of data protection law. Written or spoken communications may contain personal data as well as images,[63] including closed-circuit television (CCTV) footage[64] or sound.[65] Electronically recorded information, as well as information on paper, may be personal data; even cell samples of human tissue may be personal data, as they record the DNA of a person.

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. The processing of these special categories of data ('sensitive data') must therefore be allowed only with specific safeguards.

On the definition of sensitive data, both Convention 108 (Article 6) and the Data Protection Directive (Article 8) name the following categories:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions, religious or other beliefs; and
- personal data concerning health or sexual life.

Example: In *Bodil Lindqvist*,[66] 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 within the meaning of Article 8 (1) of Directive 95/46."

63 ECtHR, *Von Hannover v. Germany*, No. 59320/00, 24 June 2004; ECtHR, *Sciacca v. Italy*, No. 50774/99, 11 January 2005.

64 ECtHR, *Peck v. the United Kingdom*, No. 44647/98, 28 January 2003; ECtHR, *Köpke v. Germany*, No. 420/07, 5 October 2010.

65 Data Protection Directive, Recitals 16 and 17; ECtHR, *P.G. and J.H. v. the United Kingdom*, No. 44787/98, 25 September 2001, paras. 59 and 60; ECtHR, *Wisse v. France*, No. 71611/01, 20 December 2005.

66 CJEU, C-101/01, *Bodil Lindqvist*, 6 November 2003, para. 51.

The Data Protection Directive additionally lists 'trade union membership' as sensitive data, as this information can be a strong indicator of political belief or affiliation.

Convention 108 also considers personal data relating to criminal convictions as sensitive.

Article 8 (7) of the Data Protection Directive mandates EU Member States "to determine the conditions under which a national identification number or any other identifier of general application may be processed."

2.1.3. Anonymised and pseudonymised data

According to the principle of limited retention of data, contained in the Data Protection Directive as well as in Convention 108 (and 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 data were collected or for which they are further processed."[67] Consequently, data would have to be anonymised if a controller wanted to store them after they were outdated and no longer served their initial purpose.

Anonymised data

Data are anonymised if all identifying elements have been eliminated from a set of personal data. No element may be left in the information which could, by exercising reasonable effort, serve to re-identify the person(s) concerned.[68] Where data have been successfully anonymised, they are no longer personal data.

If personal data no longer serve their initial purpose, but are to be kept in a personalised form for the purpose of historical, statistical or scientific use, the Data Protection Directive and Convention 108 allow this possibility on condition that appropriate safeguards against misuse are applied.[69]

67 Data Protection Directive, Art. 6 (1) (e); and Convention 108, Article 5 (e).

68 *Ibid.*, Recital 26.

69 *Ibid.*, Art. 6 (1) (e); and Convention 108, Article 5 (e).

Pseudonymised data

Personal information contains identifiers, such as a name, date of birth, sex and address. When personal information is pseudonymised, the identifiers are replaced by one pseudonym. Pseudonymisation is achieved, for instance, by encryption of the identifiers in personal data.

Pseudonymised data are not explicitly mentioned in the legal definitions of either Convention 108 or the Data Protection Directive. However, the Explanatory Report to Convention 108 states in its Article 42 that "[t]he requirement [...] concerning the time-limits for the storage of data in their name-linked form does not mean that data should after some time be irrevocably separated from the name of the person to whom they relate, but only that it should not be possible to link readily the data and the identifiers". This is an effect which can be achieved by pseudonymising the data. For everyone who is not in possession of the decryption key, pseudonymised data can be identifiable with difficulty. The link to an identity still exists in form of the pseudonym plus the decryption key. For those who are entitled to use the decryption key re-identification is easily possible. Use of encryption keys by unauthorised persons must be particularly guarded against.

As pseudonymisation of data is one of the most important means of achieving data protection on a large scale, where it is not possible to entirely refrain from using personal data, the logic and the effect of such action must be explained in more detail.

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:

"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

"YESz320l is the father of a family of four children, two boys and two girls".

Users who access these pseudonymised data will usually have no ability to identify "Charles Spencer, born 3 April 1967" from "324" or "YESz3201". Pseudonymised 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 method of pseudonymisation affects the effectiveness of data protection.

Personal data with encrypted identifiers are used in many contexts as a means to keep secret the identity of persons. 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 advanced data-processing systems.

2.2. Data processing

Key points

- The term 'processing' refers primarily to automated processing.
- Under EU law, 'processing' refers additionally to manual processing in structured filing systems.
- Under CoE law, the meaning of 'processing' can be extended by domestic law to include manual processing.

Data protection under Convention 108 and the Data Protection Directive is primarily focused on automated data processing.

Under **CoE law**, the definition of automatic processing recognises, however, that some stages of manual use of personal data may be required between automated operations. Similarly, under **EU law**, automated data processing is defined as "operations performed upon personal data, in whole or in part by automatic means".[70]

70 Convention 108, Art. 2 (c); and Data Protection Directive, Art. 2 (b) and Art. 3 (1).

Example: In *Bodil Lindqvist*,[71] 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."

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 the processing of personal data in a manual filing system, that is, a specially structured paper file.[72] 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; and
- storing personal data in structured paper files makes it easy to circumvent the restrictions laid down by law for automated data processing.[73]

Under CoE law, Convention 108 primarily regulates data processing in automated data files.[74] It also provides, however, for the possibility of extending protection to manual processing in domestic law. Many Parties to Convention 108 have made use of this possibility and made declarations to this end to the CoE Secretary General.[75] Extension of data protection under such a declaration must pertain to all manual data processing and cannot be limited to processing in manual filing systems.[76]

As for the nature of processing operations included, the concept of processing is comprehensive **under both EU and CoE law**: "'processing of personal data' [...] shall mean any operation [...] such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

71 CJEU, C-101/01, *Bodil Lindqvist*, 6 November 2003, para. 27.

72 Data Protection Directive, Art. 3 (1).

73 *Ibid.*, Recital 27.

74 Convention 108, Art. 2 (b).

75 See the declarations made under Convention 108, Art. 3 (2) (c).

76 See the wording of Convention 108, Art. 3 (2).

dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction"[77] performed upon personal data. The term 'processing' also includes actions whereby the data leave the responsibility of one controller and are transferred to the responsibility of another controller.

Example: Employers collect and process data about their employees, including information relating to their salaries. The legal ground for legitimately doing so is the labour contract.

Employers will have to forward their staff's salary data to the tax authorities. This forwarding of data will also be 'processing' under the meaning of this term in Convention 108 and in the directive. The legal ground, however, for such disclosure is not the labour contract. There must be an additional legal basis for the processing operations which result in the transfer of salary data from the employer to the tax authorities. This legal basis is usually contained in the provisions of national tax laws. Without such provisions, transferring data would be illegal processing.

2.3. The users of personal data

Key points

- Whoever decides to process 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 legally separate entity that processes personal data on behalf of a controller.
- A processor becomes a controller if he or she uses data for his or her own purposes, not following the instructions of a controller.
- Anybody who receives data from a controller is a 'recipient'.
- A 'third party' is a natural or legal person who does not act under instructions of the controller (and is not the data subject).
- A 'third party recipient' is a person or entity that is legally separate from the controller, but receives personal data from the controller.

77 Data Protection Directive, Art. 2 (b). Similarly, see also Convention 108, Art. 2 (c).

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. Only those who can be held responsible under the applicable law can therefore assume these positions. In the private sector, this is usually a natural or legal person; in the public sector, it is usually an authority. Other entities, such as bodies or institutions without legal personality, can be controllers or processors only where special legal provisions so provide.

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

In groups of companies, the parent company and each affiliate, being separate legal persons, count as separate controllers or processors. As a consequence of this legally separate status, the transfer of data between the members of a group of companies will need a special legal basis. There is no privilege permitting the exchange of personal data as such between the separate legal entities within the company group.

The role of private individuals needs to be mentioned in this context. **Under EU law**, private individuals, when processing data about others in the course of a purely personal or household activity, do not fall under the rules of the Data Protection Directive; they are not deemed to be controllers.[78]

However, jurisprudence has found that data protection law will, nevertheless, apply when a private person, in the course of using the internet, publishes data about others.

Example: The CJEU maintained in *Bodil Lindqvist*[79] 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

78 Data Protection Directive, Recital 12 and Art. 3 (2) last indent.

79 CJEU, C-101/01, *Bodil Lindqvist*, 6 November 2003.

data wholly or partly by automatic means' within the meaning of Article 3 (1) of Directive 95/46."[80]

Such personal data processing does not fall under purely personal or domestic activities, which are outside the scope of the Data Protection Directive, 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."[81]

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".[82] A controller's decision lays down why and how data shall be processed. **Under CoE law**, the definition of 'controller' mentions additionally that a controller decides which categories of personal data should be stored.[83]

Convention 108 refers in its definition of a controller to a further aspect of controllership which requires consideration. This definition refers to the question of who may lawfully process certain data for a certain purpose. However, where allegedly illegal processing operations take place and the responsible controller must be found, it will be the person or entity, such as a company or an authority, who decided that the data should be processed, irrespective of whether it was legally entitled to do so or not[84] that will be considered the controller. A request for deletion must therefore always be addressed to the 'factual' controller.

Joint controllership

The definition of 'controller' in the Data Protection Directive provides that there might also be several legally separate entities who together or jointly with others act as controller. This means that they decide together to process data for a shared

80 *Ibid.*, para. 27.

81 *Ibid.*, para. 47.

82 Data Protection Directive, Art. 2 (d).

83 Convention 108, Art. 2 (d).

84 See also Article 29 Working Party (2010), *Opinion 1/2010 on the concepts of 'controller' and 'processor'*, WP 169, Brussels, 16 February 2010, p. 15.

purpose.[85] This is legally possible, however, only in cases where a special legal basis provides for processing the data jointly for a common purpose.

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.

Regulations 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. However, no relevant jurisprudence is yet available at the European level and there is also no clarity about the consequences concerning liability. The Article 29 Working Party advocates a broader interpretation of the concept of joint controllership with the aim of allowing some flexibility in order to cater for the increasing complexity of current data-processing reality.[86] 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.[87] SWIFT had, by deciding about disclosure, assumed – unlawfully – the role of controller; the banking institutions had evidently fallen short of their obligation to supervise their processor and therefore could not be completely absolved from their responsibility as controllers. This situation results in joint controllership.

85 Data Protection Directive, Art. 2 (d).

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

87 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.

Processor

A processor is defined **under EU law** as someone who processes personal data on behalf of a controller.[88] 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.

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, e.g. the administration of their own employees, sales and accounts.

Examples: 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.

The 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.

Example: The director of the Sunshine company decides that the Moonlight company, a specialist in market analysis, should conduct a market analysis of Sunshine's customer data. Although the task of determining the means of processing will thus be delegated to Moonlight, the Sunshine company remains the controller and Moonlight is only a processor, as, according to the contract, Moonlight may use the customer data of the Sunshine company only for the purposes Sunshine determines.

If the power to determine the means of processing is delegated to a processor, the controller must nonetheless be able to interfere with the decisions of the processor regarding the means of processing. Overall responsibility still lies with the controller,

88 Data Protection Directive, Art. 2 (e).

who must supervise the processors to ensure that their decisions comply with data protection law. A contract forbidding the controller to interfere with the decisions of the processor would, therefore, probably be construed as resulting in joint controllership, with both parties sharing the legal responsibility of a controller.

Furthermore, should a processor not honour the limitations of data use as prescribed by the controller, the processor will have become a controller at least to 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. 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.[89] An important consequence of joint controllership should be joint and several liability for damages, affording the data subjects a wider range of remedies.

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.[90]

For the sake of clarity and transparency, the details of the relationship between a controller and a processor should be recorded in a written contract.[91] Having no such contract is an infringement of the controller's obligation to provide written documentation of mutual responsibilities, and could lead to sanctions.[92]

Processors might want to delegate certain tasks to additional sub-processors. This is legally permissible and will depend in detail on the contractual stipulations between the controller and the processor, including whether the controller's authorisation is necessary in every single case, or whether informing alone is sufficient.

89 Article 29 Working Party (2010), *Opinion 1/2010 on the concepts of 'controller' and 'processor'*, WP 169, Brussels, 16 February 2010, p. 25; and 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.

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

91 Data Protection Directive, Art. 17 (3) and (4).

92 Article 29 Working Party (2010), *Opinion 1/2010 on the concepts of 'controller' and 'processor'*, WP 169, Brussels, 16 February 2010, p. 27.

Under CoE law, the interpretation of the concepts of controller and processor, as explained above, is fully applicable, as is demonstrated by the recommendations which have been developed pursuant to Convention 108.[93]

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 legally different from the controller. Disclosing data to a third party will, therefore, always need a specific legal basis. According to Article 2 (f) of the Data Protection Directive, a third party is "any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data". This means that persons working for an organisation which is legally 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'.[94]

'Recipient' is a broader term than 'third party'. In the meaning of Article 2 (g) of the Data Protection Directive, a recipient means "a natural or legal person, public authority, agency or any other body to whom 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 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 without further legal requirement be recipients of personal data if they are involved in the processing operations of the controller or processor. On the other hand, a third party, being legally separate from the controller or processor, is not authorised to use personal data processed by the controller, unless on specific legal

93 See, for example, Profiling Recommendation, Art. 1.

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

grounds in a specific case. 'Third-party recipients' of data will, therefore, always need a legal basis for lawfully receiving personal data.

Example: A processor'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 processor.

If, however, the same employee decides to use the data, which he or she is able to access as an employee of the processor, for his or her own purposes and sells them to another company, then the employee has acted as a third party. He or she is no longer following the orders of the processor (the employer). As a third party, the employee would need a legal basis for acquiring and selling the data. In this example, the employee certainly does not possess such a legal basis, so these actions are illegal.

2.4. Consent

Key points

- Consent as a legal basis for processing personal data must be free, informed and specific.
- Consent must have been given unambiguously. Consent may either be given explicitly or implied by acting in a way which leaves no doubt that the data subject agrees to the processing of his or her data.
- Processing sensitive data on the basis of consent requires explicit consent.
- Consent can be withdrawn at any time.

Consent means "any freely given specific and informed indication of the data subject's wishes."[95] It is, in numerous cases, the legal basis for legitimate data processing (see Section 4.1).

95 Data Protection Directive, Art. 2 (h).

2.4.1. The elements of valid consent

EU law sets out three elements for consent to be valid, which aim to guarantee that data subjects truly meant to agree to the use of their data:

- the data subject must have been under no pressure when consenting;
- the data subject must have been duly informed about the object and consequences of consenting; and
- the scope of consent must be reasonably concrete.

Only if all of these requirements are fulfilled will consent be valid in the sense of the data protection law.

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, as it is provided by the recommendations which have been developed pursuant to Convention 108.[96] The requirements for consent are the same as for a valid declaration of intention under European civil law.

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.

The consent can be given either explicitly[97] or non-explicitly. The former leaves no doubt about the intentions of the data subject and can be made either orally or in writing; the latter is concluded from the circumstances. Every consent must be given in an unambiguous way.[98] This means that there should be no reasonable doubt that the data subject wanted to communicate his or her agreement to allow processing of his or her data. Deducing consent from mere inactivity is not capable of delivering unambiguous consent, for example. Where data to be processed are sensitive, explicit consent is mandatory and must be unambiguous.

96 See, for example, Convention 108, Statistical Data Recommendation, point 6.

97 Data Protection Directive, Art. 8 (2).

98 *Ibid.*, Art. 7 (a) and Art. 26 (1).

Free consent

The existence of free consent is valid only "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".[99]

Example: In many airports, passengers need to go through body scanners in order to enter the boarding area.[100] Given that passengers' data are processed during scanning, the processing must comply with one of the legal grounds under Article 7 of the Data Protection Directive (see Section 4.1.1). Going through body scanners is sometimes presented to passengers as an option, implying that their consent could justify the processing. Passengers might, however, fear that their refusal to go through body scanners will create suspicion, or trigger additional controls, such as body searches. Many passengers consent to being scanned because by so doing they avoid potential problems or delays. Such consent is presumably not sufficiently free.

Therefore, a sound legitimate basis can only be found in an act of the legislator, based on Article 7 (e) of the Data Protection Directive, resulting in an obligation for passengers to cooperate because of overriding public interest. Such legislation could still provide for a choice between scanning and pat-down, but only as part of additional measures of border control necessary under particular circumstances. This is what the European Commission set out in two regulations covering security scanners in 2011.[101]

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

100 This example is taken from *Ibid.*, p. 15.

101 Commission Regulation (EU) No. 1141/2011 of 10 November 2011 amending Regulation (EC) No. 272/2009 supplementing the common basic standards on civil aviation security as regards the use of security scanners at EU airports, OJ 2011 L 293, and Commission Implementing Regulation (EU) No. 1147/2011 of 11 November 2011 amending Regulation (EU) No. 185/2010 implementing the common basic standards on civil aviation security as regards the use of security scanners at EU airports, OJ 2011 L 294.

Free consent could also be threatened in situations of subordination where there is a significant economic or other imbalance between the controller securing consent and the data subject providing consent.[102]

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, for example, 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 clear that having a photo published in the directory does not have negative consequences in itself and, moreover, it is credible that the employee will not have to encounter negative effects initiated by the employer if he or she does not agree to have his or her photo published in the directory.

This does not mean, however, that consent can never be valid in circumstances where not consenting would have negative consequences. If, for instance, not consenting to having a supermarket's customer card results only in not receiving deductions from prices of certain goods, consent is still a valid legal basis for processing personal data of those customers who consented to having such a card. There is no situation of subordination between company and customer and, the consequences of not consenting are not serious enough for the data subject to prevent free choice.

On the other hand, whenever sufficiently important goods or services can be obtained only and exclusively if certain personal data are disclosed to third parties, consent of the data subject to the disclosure of his or her data can usually not be considered a free decision and is, therefore, not valid under data protection law.

Example: Agreement expressed by passengers to an airline that it transfers so-called passenger name records (PNR), namely data about their identity, eating habits or health problems to the immigration authorities of a specific foreign

102 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; and 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.

country cannot be considered as 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 transferred lawfully, another legal basis than consent is required: most likely a special law.

Informed consent

The data subject must have sufficient information before taking his or her decision. Whether or not the information given is sufficient can be decided only on a case-by-case basis. Usually, informed consent will comprise a precise and easily understandable description of the subject matter requiring consent and, additionally, outline the consequences of consenting or not consenting. The language used for information should be adapted to the foreseeable addressees of the information.

Information must also be easily available to the data subject. Accessibility and visibility of the information are important elements. In an online environment, layered information notices may be a good solution, as, in addition to a concise version of information, a more extensive version can also be accessed by the data subject.

Specific consent

To be valid, consent must also be specific. This goes hand in hand with the quality of information given about the object of 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 reasonably have been foreseen when the initial consent was given.

Example: In *Deutsche Telekom AG*,[103] the CJEU dealt with the question of whether a telecom provider that had to pass on personal data of subscribers under Article 12 of the *Directive on privacy and electronic communications*[104] needed renewed consent from the data subjects, as the recipients were not originally named when consent was given.

103 CJEU, C-543/09, *Deutsche Telekom AG v. Germany*, 5 May 2011; see especially paras. 53 and 54.

104 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*).

The CJEU held that under that article renewed consent before passing on the data was not necessary because the data subjects had, under this provision, the possibility of consenting only to the purpose of the processing, which is the publication of their data, and could not choose between different directories in which these data might be published.

As the Court 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."[105] Moreover, "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"[106]and not who is the author of this publication.

2.4.2. The right to withdraw consent at any time

The Data Protection Directive does not mention a general right to withdraw consent at any time. It is widely presumed, however, that such a right exists and that it must be possible for the data subject to exercise it 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.

Example: A customer agrees to receive 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.

If the customer was receiving a 5 % reduction on the cost of a hotel room in return for agreeing to the use of his or her data for promotional mail, the withdrawal of consent to receiving promotional mail at a later stage should not result in having to pay back those reductions.

105 CJEU, C-543/09, *Deutsche Telekom AG v. Germany*, 5 May 2011; see especially para. 61.

106 *Ibid.*, see especially para. 62.

3 The key principles of European data protection law

EU	Issues covered	CoE
Data Protection Directive, Article 6 (1) (a) and (b) CJEU, C-524/06, *Huber v. Germany*, 16 December 2008 CJEU, Joined cases C-92/09 and C-93/09, *Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, 9 November 2010	**The principle of lawful processing**	Convention 108, Article 5 (a) and (b) ECtHR, *Rotaru v. Romania* [GC], No. 28341/95, 4 May 2000 ECtHR, *Taylor-Sabori v. the United Kingdom*, No. 47114/99, 22 October 2002 ECtHR, *Peck v. the United Kingdom*, No. 44647/98, 28 January 2003 ECtHR, *Khelili v. Switzerland*, No. 16188/07, 18 October 2011 ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987
Data Protection Directive, Article 6 (1) (b)	**The principle of purpose specification and limitation**	Convention 108, Article 5 (b)
	The data quality principles:	
Data Protection Directive, Article 6 (1) (c)	**Relevancy of data**	Convention 108, Article 5 (c)
Data Protection Directive, Article 6 (1) (d)	**Accuracy of data**	Convention 108, Article 5 (d)

Data Protection Directive, Article 6 (1) (e)	**Limited retention of data**	Convention 108, Article 5 (e)
Data Protection Directive, Article 6 (1) (e)	**Exemption for scientific research and statistics**	Convention 108, Article 9 (3)
Data Protection Directive, Article 6 (1) (a)	**The principle of fair processing**	Convention 108, Article 5 (a) ECtHR, *Haralambie v. Romania*, No. 21737/03, 27 October 2009 ECtHR, *K.H. and Others v. Slovakia*, No. 32881/04, 28 April 2009
Data Protection Directive, Article 6 (2)	**The principle of accountability**	

The principles set out in Article 5 of Convention 108 enshrine the essence of European data protection law. They appear also in Article 6 of the Data Protection Directive as the starting point for more detailed provisions in the subsequent articles of the directive. 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. Any exemptions from and restrictions to these key principles may be provided for at national level;[107] they must be provided for by law, pursue a legitimate aim and be necessary in a democratic society. All three conditions must be fulfilled.

3.1. The principle of lawful processing

Key points

- In order to understand the principle of lawful processing, one has to refer to conditions for lawful limitations of the right to data protection in light of Article 52 (1) of the Charter and requirements of justified interference under Article 8 (2) ECHR.
- Accordingly, the processing of personal data is lawful only if it:
  - is in accordance with the law; and
  - pursues a legitimate purpose; and
  - is necessary in a democratic society in order to achieve the legitimate purpose.

107 Convention 108, Art. 9 (2); Data Protection Directive, Art. 13 (2).

Under EU and CoE data protection law, the principle of lawful processing is the first named principle; it is expressed in nearly identical terms in Article 5 of Convention 108 and in Article 6 of the Data Protection Directive.

Neither of these provisions contains a definition of what constitutes 'lawful processing'. In order to understand this legal term, it is necessary to refer to justified interference under the ECHR as interpreted by the jurisprudence of the ECtHR and conditions for lawful limitations under Article 52 of the Charter.

3.1.1. The requirements for a justified interference under the ECHR

The processing of personal data may constitute an interference with the right to respect for private life of the data subject. The right to respect for private life is, however, not an absolute right but must be balanced against and reconciled with other legitimate interests, be they of other persons (private interests) or of society as a whole (public interests).

The conditions upon which state interference is justified are the following.

In accordance with the law

According to the jurisprudence of the ECtHR, interference is in accordance with the law if it is based on a provision of domestic law, which has certain qualities. The law must be "accessible to the persons concerned and foreseeable as to its effects".[108] 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".[109] "The degree of precision required of 'the law' in this connection will depend on the particular subject-matter."[110]

108 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.

109 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.

110 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.

Example: In *Rotaru v. Romania*,[111] the ECtHR found a violation of Article 8 of the ECHR because Romanian law allowed for gathering, recording and archiving in secret files of information affecting national security without laying down 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. Because of these deficiencies, the Court concluded that domestic law did not comply with the requirement of foreseeability under Article 8 of the ECHR and that that Article had been violated.

Example: In *Taylor-Sabori v. the United Kingdom*,[112] the applicant had been the target of surveillance by the police. Using a 'clone' of the applicant's pager, the police were able to intercept messages sent to him. The applicant was then 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 had been transcribed by the police. 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 there had been a violation of Article 8 of the ECHR.

Pursuing a legitimate aim

The legitimate aim may be either one of the named public interests or the rights and freedoms of others.

Example: In *Peck v. the United Kingdom*,[113] the applicant attempted suicide on the street by cutting his wrists, unaware that a CCTV camera had filmed him during the attempt. After police, who were watching the CCTV cameras, rescued him, the police authority passed the CCTV footage to the media which published it without masking the applicant's face. The ECtHR found that there were no

111 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.

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

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

relevant or sufficient reasons which 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.

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".[114]

Example: In *Khelili v. Switzerland*,[115] 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, might under 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 *Leander v. Sweden*,[116] the ECtHR ruled that secret scrutiny of persons 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

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

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

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

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.

3.1.2. The conditions for lawful limitations under the EU Charter

The structure and wording of the Charter is different from that of the ECHR. The Charter does not talk about interferences with guaranteed rights but it 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, such as the processing of personal data, are admissible only if they:

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

Examples: In *Volker and Markus Schecke*,[117] 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,

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

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.[118]

In spite of the different wording, conditions for lawful processing in Article 52 (1) of the Charter are reminiscent of Article 8 (2) of the ECHR. Indeed, the conditions enumerated in Article 52 (1) of the Charter must be seen to comply with those named in Article 8 (2) of the ECHR, as Article 52 (3) of the Charter states, in its first sentence, that, "in so far as the 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, pursuant to the last sentence of Article 52 (3), "this provision shall not prevent Union law providing more extensive protection." In the context of comparing Article 8 (2) of the ECHR and the first sentence of Article 52 (3), this can only mean that the conditions for justified interferences according to Article 8 (2) of the ECHR are the minimum requirements for the lawful limitations of the right to data protection according to the Charter. Consequently, lawful processing of personal data requires under EU law that the conditions of Article 8 (2) of the ECHR at the least be fulfilled; EU law could, however, lay down additional requirements for specific cases.

Correspondence of the principle of lawful processing under EU law with the relevant provisions of the ECHR is further promoted by Article 6 (3) of the TEU, providing that "fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms [...], shall constitute general principles of the Union's law".

118 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.

3.2. The principle of purpose specification and limitation

Key points

- The purpose of processing data must be visibly defined before processing is started.
- Under EU law, the purpose of processing must be explicitly defined; under CoE law, this question is left to domestic law.
- Processing for undefined purposes is not compliant with data protection law.
- Further use of data for another purpose needs an additional legal basis if the new purpose of processing is incompatible with the original one.
- Transfer of data to third parties is a new purpose needing an additional legal basis.

In essence, the principle of purpose specification and limitation means that the legitimacy of processing personal data will depend on the purpose of the processing.[119] The purpose must have been specified and made manifest by the controller before the processing of data starts.[120] **Under EU law**, this must be done either by declaration, in other words by notification, to the appropriate supervisory authority or, at the least, by internal documentation which must be made available by the controller for inspection by the supervisory authorities and access by the data subject.

The processing of personal data for undefined and/or unlimited purposes is unlawful.

Every new purpose for processing data 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. Disclosure of data to third parties will have to be considered especially carefully, as disclosure will usually constitute a new purpose and therefore require a legal basis, distinct from the one for collecting the data.

119 Convention 108, Art. 5 (b); Data Protection Directive, Art. 6 (1) (b).

120 See also Article 29 Working Party (2013), *Opinion 03/2013 on purpose limitation*, WP 203, Brussels, 2 April 2013.

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 transfer these data, which are contained in the PNR, 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. Transfer 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, Convention 108 and the Data Protection Directive resort to the concept of compatibility: the use of data for compatible purposes is allowed on the ground of the initial legal basis. What 'compatible' means, however, is not defined and is left open to interpretation on a case-by-case basis.

Example: I Selling the Sunshine company's customer data, which it acquired in the course of customer relations management (CRM), to a direct marketing company, the Moonlight company, which wants to use these data to assist the marketing campaigns of third companies, is a new purpose, which is incompatible with CRM, the Sunshine company's initial purpose for collecting the customer data. The sale of the data to the Moonlight company therefore needs its own legal basis.

In 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 Data Protection Directive explicitly declares that the "further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards".[121]

Examples: The Sunshine company has collected and stored 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

121 An example of such national provisions is the Austrian Data Protection Act (*Datenschutzgesetz*), Federal Law Gazette No. 165/1999, para. 46, available in English at: www.dsk.gv.at/DocView.axd?CobId=41936.

are a compatible purpose. No additional legal basis, such as consent of the data subjects, is needed.

If the same data were to be passed on to a third party, the Starlight company, for exclusively statistical purposes, passing on would be permissible without additional legal basis, but only on the condition that appropriate safeguards were in place, such as masking the identity of the data subjects, as identities are usually not needed for statistical purposes.

3.3. Data quality principles

Key points

- The principles of data quality must be implemented by the controller in all processing operations.
- The principle of limited retention of data makes it necessary to delete data as soon as they are no longer needed for the purposes for which they were collected.
- Exemptions from the principle of limited retention must be set out by law and need special safeguards for the protection of data subjects.

3.3.1. The data relevancy principle

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".[122] 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.

In contemporary society, the principle of data relevancy has an additional consideration: by making use of special privacy-enhancing technology, it is sometimes possible to avoid using personal data at all, or to use pseudonymised data, which results in a privacy-friendly solution. This is particularly appropriate in more extensive processing systems.

122 Convention 108, Art. 5 (c); and Data Protection Directive, Art. 6 (1) (c).

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 relevancy 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. No personal data would be collected, which is the optimal solution in the sense of the relevancy principle, as this principle results in the obligation to minimise data collection.

3.3.2. The data accuracy principle

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.

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

Example: A furniture sales company collected a customer's identity and address data in order to bill him or her. Six months later, the same company wants to start a marketing campaign and wishes to contact former customers. In order to reach them, the company wants to access the national residents' register, which is likely to contain updated addresses, as residents are legally obliged to inform the register of their current address. Access to the data of this register is limited to persons who, and entities that, can provide a justifying reason.

In this situation, the company cannot use the argument that data must be kept accurate and up to date to maintain that it is entitled to collect new address

data on all its former customers from the residents' register. The data were collected in the course of billing; for this purpose, the address at the time of sale is relevant. There is no legal basis for collecting new address data, as marketing is not an interest which overrides the right to data protection and therefore cannot justify accessing the register's data.

There may also be cases where updating stored data is legally prohibited, because the purpose of storing the data is principally to document events.

Example: A medical operation protocol must not be changed, in other words 'updated', even if findings mentioned in the protocol later on turn out to have been wrong. In such circumstances, only additions to the remarks in the protocol 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 regular checking of the accuracy of data, including updating, is an absolute necessity because of the potential damage which might be caused to the data subject if data were to remain inaccurate.

Example: If somebody wants to conclude a 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 encounter serious problems. Controllers of such databases must therefore make special efforts to follow the principle of accuracy.

Further, data which relate not to facts, but to suspicions, such as criminal investigations, may be collected and stored as long as the controller has a legal basis for collecting such information and is sufficiently justified in having formed such a suspicion.

3.3.3. The limited retention of data principle

Article 6 (1) (e) of the Data Protection Directive and, likewise, Article 5 (e) of Convention 108 require Member States to ensure that personal data are "kept in a form which permits identification of data subjects for no longer than is necessary for the

purposes for which the data were collected or for which they are further processed." The data must therefore be erased when those purposes have been served.

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 retention of data to be proportionate in relation to the purpose of collection and limited in time, particularly in the police sector.[123]

The time limitation for storing personal data applies, however, only 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 anonymisation of the data or pseudonymisation.

Keeping data for future scientific, historical or statistical use is explicitly exempt from the principle of limited data retention in the Data Protection Directive.[124] Such ongoing storage and use of personal data must, however, be accompanied by special safeguards under national law.

3.4. The fair processing principle

Key points

- Fair processing means transparency of processing, especially *vis-à-vis* data subjects.
- Controllers must inform data subjects before processing their data, at least about the purpose of processing and about the identity and address of the controller.
- Unless specifically permitted by law, there must be no secret and covert processing of personal data.
- Data subjects have the right to access their data wherever they are processed.

The principle of fair processing governs primarily the relationship between the controller and the data subject.

123 ECtHR, *S. and Marper v. the United Kingdom*, 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.

124 Data Protection Directive, Art. 6 (1) (e).

3.4.1. Transparency

This principle establishes an obligation for the controller to keep the data subjects informed about how their data are being used.

Example: In the case of *Haralambie v. Romania*,[125] the applicant requested access to the file which the secret service organisation had stored on him, but his request was granted only five years later. 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 files transferred 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. A data subject also has the right to be told by a controller on request if his or her data are being processed, and, if so, which ones.

3.4.2. Establishing trust

Controllers should document, to data subjects and to the general public, that they will process data in a lawful and transparent manner. Processing operations must not be performed in secret and should not have unforeseeable negative effects. Controllers should ensure that customers, clients or citizens are informed about the use of their data. Further, 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 the case of *K.H. and Others v. Slovakia*,[126] the applicants were eight women of Roma ethnic origin who had been treated in two hospitals in eastern Slovakia during their pregnancies and deliveries. Afterwards, none of them

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

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

could 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 compelling reasons for refusing to do so. In the applicants' case, the domestic courts justified the prohibition on making copies of 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.

Fair processing also means that controllers are prepared to go beyond the mandatory legal minimum requirements of service to the data subject, should the legitimate interests of the data subject so require.

3.5. The principle of accountability

Key points

- Accountability requires the active implementation of measures by controllers to promote and safeguard data protection in their processing activities.
- Controllers are responsible for the compliance of their processing operations with data protection law.
- Controllers should be able at any time to demonstrate compliance with data protection provisions to data subjects, to the general public and to supervisory authorities.

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 develop 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."[127]

Whereas Convention 108 makes no reference to the accountability of controllers, essentially leaving this topic to domestic law, Article 6 (2) of the Data Protection Directive states that the controller should ensure compliance with the principles relating to data quality included in paragraph 1.

Example: A legislative example for stressing the principle of accountability is the 2009 amendment[128] to the Directive on privacy and electronic communications (2002/58/EC). According to Article 4 in its amended form, the directive imposes an obligation to implement a security policy, namely 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.

According to the Article 29 Working Party's opinion,[129] 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 proves to data subjects and to supervisory authorities what measures have been taken to achieve adherence to the data protection rules.

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

128 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, p. 11.

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

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.

4

The rules of European data protection law

EU	Issues covered	CoE
Rules on lawful processing of non-sensitive data		
Data Protection Directive, Article 7 (a)	Consent	Profiling Recommendation, Articles 3.4 (b) and 3.6
Data Protection Directive, Article 7 (b)	(Pre-)contractual relationship	Profiling Recommendation, Article 3.4 (b)
Data Protection Directive, Article 7 (c)	Legal duties of the controller	Profiling Recommendation, Article 3.4 (a)
Data Protection Directive, Article 7 (d)	Vital interests of the data subject	Profiling Recommendation, Article 3.4 (b)
Data Protection Directive, Article 7 (e) and Article 8 (4) CJEU, C-524/06, *Huber v. Germany*, 16 December 2008	Public interest and exercise of official authority	Profiling Recommendation, Article 3.4 (b)
Data Protection Directive, Article 7 (f), Article 8 (2) and 8 (3) 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	Legitimate interests of others	Profiling Recommendation, Article 3.4 (b)
Rules on lawful processing of sensitive data		
Data Protection Directive, Article 8 (1)	General prohibition to process	Convention 108, Article 6
Data Protection Directive, Article 8 (2)–(4)	Exemptions from the general prohibition	Convention 108, Article 6

Data Protection Directive, Article 8 (5)	Processing data on (criminal) convictions	Convention 108, Article 6
Data Protection Directive Article 8 (7)	Processing identification numbers	
Rules on secure processing		
Data Protection Directive, Article 17	Obligation to provide for secure processing	Convention 108, Article 7
		ECtHR, *I. v. Finland*, No. 20511/03, 17 July 2008
Directive on privacy and electronic communications, Article 4 (2)	Data breach notifications	
Data Protection Directive, Article 16	Obligation to confidentiality	
Rules on transparency of processing		
	Transparency in general	Convention 108, Article 8 (a)
Data Protection Directive, Articles 10 and 11	Information	Convention 108, Article 8 (a)
Data Protection Directive, Articles 10 and 11	Exemptions from the obligation to inform	Convention 108, Article 9
Data Protection Directive, Articles 18 and 19	Notification	Profiling Recommendation, Article 9.2 (a)
Rules on promoting compliance		
Data Protection Directive, Article 20	Prior checking	
Data Protection Directive, Article 18 (2)	Personal data protection officials	Profiling Recommendation, Article 8.3
Data Protection Directive, Article 27	Codes of conduct	

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 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 already at the EU level in order to harmonise the level of data protection of the national laws of the Member States. The Data Protection Directive establishes, under the principles set out in its Article 6, a layer of detailed rules which must be faithfully implemented in national law. The following remarks on detailed data protection rules at the European level deal, therefore, predominantly with EU law.

4.1. Rules on lawful processing

Key points

- Personal data may be lawfully processed if:
  - the processing is based on the consent of the data subject; or
  - vital interests of data subjects require the processing of their data; or
  - legitimate interests of others are the reason for processing, but only as long as they are not overridden by interests in protecting the fundamental rights of the data subjects.
- Lawful processing of sensitive personal data is subject to a special, stricter regime.

The Data Protection Directive contains two different sets of rules for lawful processing of data: one for non-sensitive data in Article 7 and one for sensitive data in Article 8.

4.1.1. Lawful processing of non-sensitive data

Chapter II of Directive 95/46, entitled 'General rules on the lawfulness of the processing of personal data', provides that, subject to the exceptions permitted under Article 13, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the Data Protection Directive and, secondly, with one of the criteria for making data processing legitimate, listed in Article 7.[130] This explains the cases which legitimise the processing of non-sensitive personal data.

Consent

Under CoE law, consent is not mentioned in Article 8 of the ECHR or in Convention 108. It is, however, mentioned in the ECtHR jurisprudence and several CoE recommendations. **Under EU law**, consent as a basis for legitimate data processing is

130 CJEU, Joined cases C-465/00, C-138/01 and C-139/01. *Rechnungshof v. Österreichischer Rundfunk and Others and Neukomm and Lauermann v. Österreichischer Rundfunk*, 20 May 2003, para. 65; CJEU, C-524/06, *Huber v. Germany*, 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.

firmly established in Article 7 (a) of the Data Protection Directive and is also explicitly mentioned in Article 8 of the Charter.

Contractual relationship

Another basis for legitimate processing of personal data **under EU law**, enumerated in Article 7 (b) of the Data Protection Directive, is if it is "necessary for the performance of a contract to which the data subject is party". This provision also covers precontractual relationships. For instance: 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 "in order to take steps at the request of the data subject prior to entering into a contract".

As concerns CoE law, "the protection of the rights and freedoms of others" is mentioned in Article 8 (2) of the ECHR as a reason for legitimate interference with the right to data protection.

Legal duties of the controller

EU law then explicitly mentions another criterion for making data processing legitimate, namely if "it is necessary for compliance with a legal obligation to which the controller is subject" (Article 7 (c) of the Data Protection Directive). This provision refers to controllers acting in the private sector; the legal obligations of public sector data controllers fall under Article 7 (e) of the directive. There are many cases in which private sector controllers are obliged by law to process data about others; e.g. physicians and hospitals have the legal duty to store data about the treatment of patients for several years, employers must process data about their employees for reasons of social security and taxation and businesses must process data about their customers for reasons of taxation.

In the context of the mandatory transfer of passenger data by airlines to foreign immigration control authorities, the question arose of whether or not legal obligations under *foreign* law could form a legitimate basis to process data under EU law (this issue is discussed in more detail in Section 6.2.).

Legal obligations of the controller serve as a basis for legitimate data processing also **under CoE law.** As has been pointed out before, legal obligations of a private sector

controller are just one specific case of legitimate interests of others, as mentioned in Article 8 (2) of the ECHR. The above example is, therefore, also relevant for CoE law.

Vital interests of the data subject

Under EU law, Article 7 (d) of the Data Protection Directive provides that the processing of personal data is lawful if it "is necessary in order to protect the vital interests of the data subject". Such interests, which are closely related to the survival of the data subject, could be the basis for the legitimate use of health data or of data about missing persons, for example.

Under CoE law, vital interests of the data subject are not mentioned in Article 8 of the ECHR as a reason for legitimate interference with the right to data protection. In some of the CoE recommendations complementing Convention 108 in particular fields, however, vital interests of the data subject are explicitly mentioned as a basis for legitimate data processing.[131] Vital interests of the data subject are evidently considered to be implied in the set of reasons justifying data processing: fundamental rights protection should never endanger the vital interests of the person who is protected.

Public interest and exercise of official authority

Given the many possible ways of organising public affairs, Article 7 (e) of the Data Protection Directive 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 or in a third party to whom the data are disclosed [...]".[132]

> Example: In *Huber v. Germany*,[133] 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

131 Profiling Recommendation, Art. 3.4 (b).

132 See Data Protection Directive, Recital 32.

133 CJEU, C-524/06, *Huber v. Germany*, 16 December 2008.

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 holds first that, under Article 7 (e) of the directive, personal data may lawfully be processed only 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 Court, "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 [...] 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".[134]

The Court notes that the right of free movement of a Union citizen in the territory of a Member State of which he or she is not a national, is not unconditional but may be subject to limitations and conditions imposed by the Treaty 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 Court concludes that such a system for processing personal data complies with EU law if it contains only 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 Article 7(e) of Directive 95/46/EC.[135]

Lastly, as regards the question of the use of the data contained in the register for the purposes of fighting crime, the Court holds that this objective "necessarily involves the prosecution of crimes and offences committed, irrespective

134 *Ibid.*, para. 52.

135 *Ibid.*, paras. 54, 58, 59, 66-68.

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, this provision, as interpreted by the Court, "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."[136]

The use of personal data by authorities acting in the public arena is also subject to Article 8 of the ECHR.

Legitimate interests pursued by the controller or by a third party

The data subject is not the only one with legitimate interests. Article 7 (f) of the Data Protection Directive 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 to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection [...]".

In the following judgment, the CJEU ruled explicitly on Article 7 (f) of the directive:

Example: In *ASNEF and FECEMD*,[137] 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. 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 Court first noted that Directive 95/46/EC is intended to ensure that the level of protection of the rights and freedoms of individuals with regard to 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

136 *Ibid.*, paras. 78 and 81.

137 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.

protection in the EU.[138] 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 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 principles relating to the lawfulness of the processing of personal data to Article 7 of the Directive 95/46 or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in Article 7."[139] The Court 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 the fact 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 Court concluded that "Article 7(f) of the Directive 95/46 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."[140]

Similar formulations can be found in recommendations of the CoE. The Profiling Recommendation acknowledges the processing of personal data for purposes of profiling as legitimate, if necessary for the legitimate interests of others, "except where

138 *Ibid.*, para. 28. See Data Protection Directive, Recitals 8 and 10.

139 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. 30 and 32.

140 *Ibid.*, paras. 40, 44, 48 and 49.

such interests are overridden by the fundamental rights and freedoms of the data subjects".[141]

4.1.2. Lawful processing of sensitive data

CoE law leaves it to domestic law to lay down appropriate protection for using sensitive data, while **EU law,** in Article 8 of the Data Protection Directive, contains a detailed regime for processing categories of data that reveal: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information on health or sex life. The processing of sensitive data is prohibited in principle.[142] There is, however, an exhaustive list of enumerated exemptions to this prohibition, which can be found in Article 8 (2) and (3) of the directive. These exemptions include explicit consent of the data subject, vital interests of the data subject, legitimate interests of others and public interest.

Unlike in the case of processing non-sensitive data, a contractual relationship with the data subject is not viewed as a general basis for the legitimate processing of sensitive data. Therefore, if sensitive data are to be processed in the context of a contract with the data subject, use of these data requires the data subject's separate explicit consent, in addition to agreeing to enter into the contract. An explicit request by the data subject for goods or services which necessarily reveal sensitive data should, however, be considered to be as good as explicit consent.

Example: If an airline passenger, in the context of booking a flight, requires that the airline provide a wheelchair and kosher food, the airline is allowed to use these data even if the passenger did not sign an extra consent clause saying that he or she agrees to the use of his data revealing information about his health and religious belief.

Explicit consent of the data subject

The first condition for lawful processing of any data, regardless 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. National law may, however, provide that consenting to the use of sensitive data is not a sufficient legal basis to permit their

141 Profiling Recommendation, Art. 3.4 (b).

142 Data Protection Directive, Art. 8 (1).

processing,[143] for example, where, in exceptional cases, processing involves unusual risks for the data subject.

In one special case, even implicit consent is acknowledged as a legal basis for processing sensitive data: Article 8 (2) (e) of the directive provides that processing is not prohibited if it relates to data which are manifestly made public by the data subject. This provision evidently presumes that the action of the data subject, making his or her data public, must be interpreted as implying consent of the data subject to the use of such data.

Vital interests of the data subject

As in the case of non-sensitive data, sensitive data may be processed because of the vital interests of the data subject.[144]

For the processing of sensitive data to be legitimate on this basis, it is necessary that it was impossible to submit the question to the data subject for deciding, because, for example, the data subject was unconscious or was absent and could not be reached.

Legitimate interests of others

As in the case of non-sensitive data, the legitimate interests of others may serve as a basis for processing sensitive data. For sensitive data, and according to Article 8 (2) of the Data Protection Directive, however, this applies only to the following cases:

- where processing is necessary because of the vital interests of another person[145] where the data subject is physically or legally incapable of giving his consent;

- where sensitive data are relevant in the field of employment law, such as health data, such as in the context of a specifically dangerous work place, or data on religious beliefs, such as in the context of holidays;[146]

143 *Ibid.,* Art. 8 (2) (a).

144 *Ibid.*, Art. 8 (2) (c).

145 *Ibid.*

146 *Ibid., Art. 8 (2) (b).*

- where foundations, associations or other non-profit-seeking bodies with a political, philosophical, religious or trade union aim, process data about their members or sponsors or other interested parties (such data are sensitive because they are likely to reveal the religious or political beliefs of the individuals concerned);[147]

- where sensitive data are used in the context of legal proceedings before a court or administrative authority for the establishment, exercise or defence of a legal claim.[148]

- Moreover, according to Article 8 (3) of the Data Protection Directive where health data are used for medical examination and treatment by healthcare providers the management of these services is included in this exemption. As a special safeguard, persons are recognised as "health care providers" only if they are subject to specific professional obligations to confidentiality.

Public interest

Additionally, according to Article 8 (4) of the Data Protection Directive, Member States may introduce further purposes for which sensitive data may be processed, as long as:

- processing data is for reasons of substantial public interest; and

- it is provided for by national law or by decision of the supervisory authority; and

- the national law or decision of the supervisory authority contains the necessary safeguards in order to effectively protect the interests of the data subjects.[149]

A prominent example are electronic health file systems, which are about to be established in many Member States. Such systems permit health data, collected by health care providers in the course of treating a patient, to be 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 based

147 *Ibid., Art. 8 (2) (d).*

148 *Ibid.*, Art. 8 (2) (e).

149 *Ibid.*, Art. 8 (4).

on Article 8 (3) of the Data Protection Directive. Assuming that the existence of such electronic health file systems constitutes a substantial public interest, however, it could be based on Article 8 (4) of the directive, requiring an explicit legal basis for their establishment, which also contains the necessary safeguards to ensure that the system is run securely.[150]

4.2. Rules on security of processing

Key points

- The rules on security of processing imply an obligation of the controller and the processor to implement appropriate technical and organisational measures in order 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; and
  - the costs;
  - the sensitivity of the data processed.
- The secure processing of data is further safeguarded by the general duty on all persons, controllers or processors, to ensure that data remain confidential.

The obligation of controllers and processors to have adequate measures in place to ensure data security is, therefore, laid down in **CoE data protection law** as well as **in EU data protection law**.

4.2.1. Elements of data security

According to the relevant provisions in **EU law**:

> *"Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration,*

150 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.

unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network and against all other unlawful forms of processing".[151]

A similar provision exists under **CoE law**:

"Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination."[152]

Often, there are also industrial, national and international standards which have been developed for safe processing of data. The European Privacy Seal (EuroPriSe), for instance, is an eTEN (Trans-European Telecommunications Networks) project of the EU which has explored the possibilities of certifying products, especially software, as compliant 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.[153] ENISA regularly publishes analyses of current security threats and advice on how to address them.

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 obligations of confidentiality;

- clear distribution of responsibilities and a clear outline of competences in matters of data processing, especially regarding decisions to process personal data and to transfer data to third parties;

151 Data Protection Directive, Art. 17 (1).

152 Convention 108, Art. 7.

153 Regulation (EC) No. 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, OJ 2004 L 77.

- 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 access to personal data by electronic means and regular checks of such protocols by the internal supervisory desk;
- careful documentation for other forms of disclosure than automated access to data in order to be able to demonstrate that no illegal data transmissions have taken place.

Offering adequate data security training and education to staff members is also an important element of effective security precautions. Verification procedures must also be installed in order 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*,[154] 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.

154 ECtHR, *I. v. Finland*, No. 20511/03, 17 July 2008.

Data breach notifications

A new instrument for dealing with infringements of data security has been introduced in the data protection law of several European countries: the obligation of providers of electronic communications services to notify data breaches to the likely victims and to supervisory authorities. For telecommunications providers, this is mandatory under EU law.[155] The purpose of data breach notifications to data subjects is to avoid damage: notification of data breaches and their possible consequences minimises the risk of negative effects on the data subjects. In cases of serious negligence, the providers could also be fined.

Setting up internal procedures, in advance, for the effective management and reporting of security breaches will be necessary, as the timeframe for the obligation to report to the data subjects and/or supervisory authority, according to national law, is usually rather short.

4.2.2. Confidentiality

Under EU law, the secure processing of data is further safeguarded by the general duty on all persons, controllers or processors, to ensure that data remain confidential.

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.

155 See 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, Art. 4 (3), 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; see also 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.

Article 16 of the Data Protection Directive concerns confidentiality only within a controller–processor relationship. Whether or not controllers have to keep data confidential, in the sense that they may not disclose them to third parties, is dealt with under Articles 7 and 8 of the directive.

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, Article 16 of the Data Protection Directive does not apply, as, in fact, the use of personal data by private individuals is completely exempt from the directive's remit where such use falls within the boundaries of the so-called household exemption.[156] The household exemption is the use of personal data "by a natural person in the course of purely personal or household activity".[157] Since the CJEU's decision in the case of *Bodil Lindqvist*,[158] this exemption must, however, be interpreted narrowly, especially in regard to disclosing data. Particularly, the household exemption will not extend to the publication of personal data to an unlimited number of recipients on the internet (for more details on the case, see Sections 2.1.2, 2.2, 2.3.1 and 6.1).

Under CoE law, the obligation of confidentiality is implied in the notion of data security in Article 7 of Convention 108, which deals with data security.

For processors, confidentiality means that they may use personal data entrusted to them by the controller only in line with the instructions given by the controller. 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. Further, controllers and processors will have to take specific measures to establish for their employees a legal duty of confidentiality, normally achieved by inclusion of confidentiality clauses in the employee's employment contract.

Infringement of professional duties to confidentiality is punishable under criminal law in many EU Member States and Parties to Convention 108.

156 Data Protection Directive, Art. 3 (2) second indent.

157 *Ibid.*

158 CJEU, C-101/01, *Lindqvist*, 6 November 2003.

4.3. Rules on transparency of processing

Key points

- Before starting to process personal data, the controller must, at the very least, inform the data subjects about the identity of the controller and the purpose of the data processing, unless the data subject already has this information.
- Where the data are collected from third parties, the obligation to provide information does not apply if:
  - the data processing is provided for by law; or
  - provision of information proves impossible or would involve a disproportionate effort.
- Before starting to process personal data, the controller must, additionally:
  - notify the supervisory authority of the intended processing operations; or
  - have the processing internally documented by an independent personal data protection official, if national law provides for such proceedings.

The principle of fair processing requires transparency of processing. **CoE law** lays down, to this end, that any person must be able to establish the existence of data-processing files, their purpose and the responsible controller.[159] How this should be achieved is left to domestic law. **EU law** is more specific, securing transparency for the data subject by way of the controller's obligation to inform the data subject, and for the general public by way of notification.

Under both legal systems, exemptions and restrictions from the transparency obligations of the controller may exist in national law when such a restriction constitutes a necessary measure to safeguard certain public interests or the protection of the data subject or of the rights and freedoms of others, as long as this is necessary in a democratic society.[160] Such exemptions may, for example, be necessary in the context of investigating crime, but can also be justified in other circumstances.

159 Convention 108, Art. 8 (a).

160 *Ibid.*, Art. 9 (2); and Data Protection Directive, Art. 13 (1).

4.3.1. Information

According to CoE law as well as EU law, controllers of processing operations are obliged to inform the data subject in advance about their intended processing.[161] This obligation does not depend on a request from the data subject but must be complied with proactively by the controller, regardless of whether the data subject shows interest in the information or not.

Content of the information

The information must include the purpose of processing, as well as the identity and contact details of the controller.[162] The Data Protection Directive requires further information to be given where this "is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject". Articles 10 and 11 of the directive outline, among other things, the categories of data processed and the recipients of such data, as well as the existence of the right of access to and the right to rectify the data. Where data are collected from the data subjects, the information should clarify whether replies to the questions are obligatory or voluntary, as well as the possible consequences of a failure to reply.[163]

From the point of view of **CoE law**, the provision of such information may be considered good practice under the principle of fair data processing and is, to this extent, also part of CoE law.

The principle of fair processing requires that information be easily understandable by the 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 the intended audience is, for example, adults or children, the general public or expert academics.

Some data subjects will want to be informed only in a nutshell of how and why their data are being processed, whereas others will require a detailed explanation. How to balance this aspect of fair information is considered in an opinion of the Article 29

161 Convention 108, Art. 8 (a); and Data Protection Directive Art. 10 and 11.

162 Convention 108, Art. 8 (a); and Data Protection Directive, Art. 10 (a) and (b).

163 Data Protection Directive, Art. 10 (c).

Working Party which promotes the idea of so-called layered notices,[164] allowing the data subject to decide which level of detail he or she prefers.

Time of providing information

The Data Protection Directive contains slightly different provisions regarding the time when information has to be provided, depending on whether data are collected from the data subject (Article 10) or from a third party (Article 11). Where data are collected from the data subject, information has to be provided, at the latest, at the time of collection. Where data are collected from third parties, information has to be provided, at the latest, either at the moment the controller records the data or before the data are disclosed to a third party for the first time.

Exemptions from the obligation to inform

Under EU law, a general exemption from the obligation to inform the data subject exists where the data subject already has the information.[165] This refers to situations where the data subject will, according to the circumstances of the case, already be aware that his or her data will be processed for a certain purpose by a certain controller.

Article 11 of the directive, which relates to the obligation to inform a data subject when the data have not been obtained from him or her, also says that there will be no such obligation, in particular for processing for statistical purposes or for the purposes of historical or scientific research, where:

- the provision of such information proves impossible; or
- it would involve a disproportionate effort; or
- the recording or disclosure of the data is expressly laid down by law.[166]

Only Article 11 (2) of the Data Protection Directive states that data subjects need not be informed about processing operations if they are laid down by law. Given the

164 Article 29 Working Party (2004), *Opinion 10/2004 on More Harmonised Information Provisions*, WP 100, Brussels, 25 November 2004.

165 Data Protection Directive, Art. 10 and 11 (1).

166 *Ibid.*, Recital 40 and Article 11 (2).

general legal assumption that the law is known by its subjects, it could be argued that, where data are collected from a data subject under Article 10 of the directive, the data subject has the information. But given that knowledge of the law is only an assumption, the principle of fair processing would require under Article 10 that the data subject be informed even if processing is laid down by law, particularly as informing the data subject is not particularly burdensome where data are collected directly from the data subject.

As concerns CoE law, Convention 108 provides explicitly for exemptions from its Article 8. Again, the exemptions set out in Articles 10 and 11 of the Data Protection Directive may be seen as examples of good practice for exemptions under Article 9 of Convention 108.

Different ways of providing information

The ideal way of providing information would be to address every single data subject, orally or in writing. If the data are collected from the data subject, giving information should go hand in hand with the collection. Especially where data are collected from third parties, however, given the evident practical difficulties in reaching the data subjects personally, information can also be provided by appropriate publication.

One of the most efficient ways to provide information will be to have appropriate information clauses on the home page of the controller, such as a website privacy policy. There is, however, a significant part of the population that does not use the internet, and the information policy of a company or of a public authority ought to take this into account.

4.3.2. Notification

National law can oblige controllers to notify the competent supervisory authority of their processing operations so that these can be published. Alternatively, national law can provide that controllers may employ a personal data protection official, who is responsible in particular for keeping a register of processing operations carried out by the controller.[167] This internal register must be made available to members of the public on request.

167 *Ibid.*, Art. 18 (2) second indent.

Example: A notification, as well as documentation by an internal personal data protection official, must describe the main features of the data processing in question. This will include information about the controller, the purpose of the processing, the legal basis of the processing, the categories of data processed, the likely third party recipients and whether or not transborder data flows are intended and, if so, which ones.

The publication of notifications by the supervisory authority must be in the form of a special register. In order to fulfil its objective, access to this register ought to be easy and free of charge. The same applies to the documentation kept by a controller's personal data protection official.

Exemptions from the duties to notify the competent supervisory authority or to employ an internal data protection official may be provided by national law for processing operations which are unlikely to pose a specific risk to data subjects are listed in Article 18 (2) of the Data Protection Directive.[168]

4.4. Rules on promoting compliance

Key points

- Developing the principle of accountability, the Data Protection Directive mentions several instruments for promoting compliance:
  - prior checking of intended processing operations by the national supervisory authority;
  - personal data protection officials who shall provide the controller with special expertise in the field of data protection;
  - codes of conduct specifying the existing data protection rules for application in a branch of society, especially of business.
- CoE law proposes similar instruments for promoting compliance in its Profiling Recommendation.

168 *Ibid.*, Art. 18 (2) first indent.

4.4.1. Prior checking

According to Article 20 of the Data Protection Directive, the supervisory authority must check processing operations which may cause specific risks to the rights and freedoms of the data subjects – due to either the purpose or the circumstances of processing – before processing begins. National law must determine which processing operations qualify for prior checking. Such checking may result in processing operations being prohibited, or in an order to change features in the proposed design of the processing operations. Article 20 of the directive aims to ensure that unnecessarily risky processing does not even start, as the supervisory authority is empowered to prohibit such operations. The prerequisite for this mechanism to be effective is that the supervisory authority is indeed notified. In order to ensure that controllers fulfil their notification obligation, supervisory authorities will need coercive powers, such as the ability to fine controllers.

Example: If a company performs processing operations which, according to national law, are subject to prior checking, this company must submit documentation about the planned processing operations to the supervisory authority. The company is not allowed to start processing operations before receiving a positive response from the supervisory authority.

In some Member States, national law provides alternatively that processing operations may be started if there is no reaction from the supervisory authority within a certain timeframe, for example, three months.

4.4.2. Personal data protection officials

The Data Protection Directive allows the possibility for national law to provide that controllers may appoint an official to act as a personal data protection official.[169] The aim of such a functionary is to ensure that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.[170]

Example: In Germany, according to Section 4f, Subsection 1 of the German Federal Data Protection Act (*Bundesdatenschutzgesetz*), privately owned companies are required to appoint an internal personal data protection official if they

169 *Ibid.*, Art. 18 (2) second indent.

170 *Ibid.*

permanently employ 10 or more persons in the automated processing of personal data.

The ability to achieve this goal requires a certain amount of independence for the official's position within the controller's organisation, as is explicitly pointed out in the directive. Strong employment rights to guard against eventualities such as unjustified dismissal would also be necessary in order to support the effective functioning of this office.

In order to promote compliance with national data protection law, the concept of internal personal data protection officials has also been adopted in some of the CoE Recommendations.[171]

4.4.3. Codes of conduct

To promote compliance, business and other sectors can draw up detailed rules that govern their typical processing activities, codifying best practices. The expertise of the members of the sector will favour finding solutions which are practical and, therefore, likely to be followed. Accordingly, Member States – as well as the European Commission – are encouraged to promote the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to the directive, taking account of the specific features of the various sectors.[172]

In order to ensure that these codes of conduct are in accordance with the nationals provisions adopted pursuant to the Data Protection Directive, Member States must establish a procedure for evaluating the codes. This procedure would ordinarily require the involvement of the national authority, trade associations and other bodies representing other categories of controllers.[173]

Draft Community codes and amendments or extensions to existing Community codes may be submitted to the Article 29 Working Party for evaluation. After approval by this Working Party, the European Commission may ensure appropriate publicity for such codes.[174]

171 See, for example, the Profiling Recommendation, Art. 8.3.

172 See the Data Protection Directive, Art. 27 (1).

173 *Ibid.*, Art. 27 (2).

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

Example: The Federation of European Direct and Interactive Marketing (FEDMA) developed a European Code of Practice for the use of personal data in direct marketing. The code was successfully submitted to the Article 29 Working Party. An annex, relating to electronic marketing communications, was added to the code in 2010.[175]

175 Article 29 Working Party (2010), *Opinion 4/2010 on the European code of conduct of the FEDMA for the use of personal data in direct marketing*, WP 174, Brussels, 13 July 2010.

5 The data subject's rights and their enforcement

EU	Issues covered	CoE
Right of access		
Data Protection Directive, Article 12 CJEU, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, 7 May 2009	Right of access to one's own data	Convention 108, Article 8 (b)
	Right to rectification, erasure (deletion) or blocking	Convention 108, Article 8 (c) ECtHR, *Cemalettin Canli v. Turkey*, No. 22427/04, 18 November 2008 ECtHR, *Segerstedt-Wiberg and Others v. Sweden*, No. 62332/00, 6 June 2006 ECtHR, *Ciubotaru v. Moldova*, No. 27138/04, 27 April 2010
Right to object		
Data Protection Directive, Article 14 (1) (a)	Right to object due to the data subject's particular situation	Profiling Recommendation, Article 5.3
Data Protection Directive, Article 14 (1) (b)	Right to object to further use of data for marketing purposes	Direct Marketing Recommendation, Article 4.1
Data Protection Directive, Article 15	Right to object to automated decisions	Profiling Recommendation, Article 5.5
Independent supervision		

Charter, Article 8 (3) Data Protection Directive, Article 28 EU Institutions Data Protection Regulation, Chapter V Data Protection Regulation CJEU, C-518/07, *European Commission v. Federal Republic of Germany*, 9 March 2010 CJEU, C-614/10, *European Commission v. Republic of Austria*, 16 October 2012 CJEU, C-288/12, *European Commission v. Hungary*, 8 April 2014	**National supervisory authorities**	Convention 108, Additional Protocol, Article 1
Remedies and sanctions		
Data Protection Directive, Article 12	**Request to the controller**	Convention 108, Article 8 (b)
Data Protection Directive, Article 28 (4) EU Institutions Data Protection Regulation, Article 32 (2)	**Claims lodged with a supervisory authority**	Convention 108, Additional Protocol, Article 1 (2) (b)
Charter, Article 47	**Courts (in general)**	ECHR, Article 13
Data Protection Directive, Article 28 (3)	**National courts**	Convention 108, Additional Protocol, Article 1 (4)
TFEU, Article 263 (4) EU Institutions Data Protection Regulation, Article 32 (1) TFEU, Article 267	**CJEU**	
	ECtHR	ECHR, Article 34
Remedies and sanctions		
Charter, Article 47 Data Protection Directive, Articles 22 and 23 CJEU, C-14/83, *Sabine von Colson and Elisabeth Kamann v. Land Nordrhein-Westfalen*, 10 April 1984 CJEU, C-152/84, *M.H. Marshall v. Southampton and South-West Hampshire Area Health Authority*, 26 February 1986	**For infringements of national data protection law**	ECHR, Article 13 (only for CoE member states) Convention 108, Article 10 ECtHR, *K.U. v. Finland*, No. 2872/02, 2 December 2008 ECtHR, *Biriuk v. Lithuania*, No. 23373/03, 25 November 2008
EU Institutions Data Protection Regulation, Articles 34 and 49 CJEU, C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd*, 29 June 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 European data protection law, the data subject must be empowered by national law to protect his or her data. Independent supervisory authorities must also be established by national law to assist the data subjects in exercising their rights and to supervise the processing of personal data. Additionally, the right to an effective remedy, as guaranteed under the ECHR and the Charter, demands that judicial remedies be available to every person.

5.1. The rights of data subjects

Key points

- Everyone shall have the right under national law to request from any controller information as to whether the controller is processing his or her data.
- Data subjects shall have the right under national law to:
  - access their own data from any controller who processes such data;
  - have their data rectified (or blocked, as appropriate) by the controller processing their data, if the data are inaccurate;
  - have their data deleted or blocked, as appropriate, by the controller if the controller is processing their data illegally.
- Additionally, data subjects shall have the right to object to controllers about:
  - automated decisions (made using personal data processed solely by automatic means);
  - the processing of their data if it leads to disproportionate results;
  - the use of their data for direct marketing purposes.

5.1.1. Right of access

Under EU law, Article 12 of the Data Protection Directive contains the elements of the data subjects' right of access, including the right to obtain from the controller "confirmation as to whether or not data relating to them are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed", as well as "the rectification, erasure or blocking of data the processing of

which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data".

In CoE law, these same rights exist and must be provided for by domestic law (Article 8 of Convention 108). In several CoE recommendations, the term 'access' is used and the different aspects of the right to access are described and proposed for implementation in domestic law in the same way as pointed out in the paragraph above.

According to Article 9 of Convention 108 and Article 13 of the Data Protection Directive, the obligation of controllers to respond to a data subject's access request may be restricted as a result of the overriding legal interests of others. Overriding legal interests may involve public interests such as national security, public security and prosecuting of criminal offences, as well as private interests which are more compelling than data protection interests. 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 protection of the data subject may itself require a restriction of transparency; this relates especially to restricting the right of access of every data subject.

Whenever data are processed solely for the purpose of scientific research or for statistical purposes, the Data Protection Directive allows access rights to be restricted by national law; however, adequate legal safeguards must be in place. In particular, it must be ensured that no measures or decisions regarding any particular individual are taken in the context of such data processing and that "there is clearly no risk of breaching the privacy of the data subject".[176] Similar provisions are contained in Article 9 (3) of Convention 108.

The right of access to one's own data

Under CoE law, the right to access one's own data is explicitly acknowledged by Article 8 of the Convention 108.The ECtHR has repeatedly held that there is a right to access information about one's personal data held or used by others, and that this right arises from the need to respect private life.[177] In the case of *Leander*,[178] the

176 Data Protection Directive, Art. 13 (2).

177 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.

178 ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987.

ECtHR concluded that the right to access personal data stored by public authorities might, however, be limited in certain circumstances.

Under EU law, the right to access one's own data is explicitly acknowledged by Article 12 of the Data Protection Directive and, as a fundamental right, in Article 8 (2) of the Charter.

Article 12 (a) of the directive provides that Member States are to guarantee every data subject a right of access to their personal data and to information. In particular, every data subject has a right to obtain from the controller confirmation as to whether or not data relating to him are being processed and information covering at least the following:

- the purposes of the processing;
- the categories of data concerned;
- the data undergoing processing;
- the recipients or categories of recipients to whom the data are disclosed;
- any available information about the source of the data undergoing processing;
- in the case of automated decisions, the logic involved in any automatic processing of data.

National law may add information to be given by the controller, for instance quoting the legal basis authorising the data processing.

Example: By accessing one's personal data, one is able to determine whether or not the data are accurate. It is, therefore, indispensable that the data subject be informed about the categories of data processed as well as about the data content. It is thus insufficient for a controller to simply tell the data subject that it is processing his or her name, address, date of birth and sphere of interest. The controller must also disclose to the data subject that it is processing "the name: N.N.; an address: 1040 Vienna, Schwarzenbergplatz 11, Austria; the date of birth: 10.10.1974; and sphere of interest (according to the data subject's

declaration): classical music." The last item contains, additionally, information on the data source.

Communication to the data subject on the data undergoing processing and of any available information as to their source must be given in an intelligible form, which means that the controller may have to explain to the data subject in more detail what it is processing. For example, just quoting technical abbreviations or medical terms in response to an access request will usually not suffice, even if only such abbreviations or terms are stored.

Information about the source of data which are processed by the controller must be given in the response to an access request as far as this information is available. This provision must be understood in light of the principles of fairness and of accountability. A controller may not destroy information about the source of data in order to be exempt from disclosing it, nor may it ignore the usual standard and acknowledged needs for documentation in the area of its activities. Keeping no documentation on the source of the data processed will usually not fulfil the controller's obligations under the right of access.

Where automated evaluations are performed, the general logic of the evaluation will need to be explained, including the particular criteria which have been considered when evaluating the data subject.

The directive does not make it clear whether the right to access information concerns the past and, if so, what period in the past. In that regard, as underlined in the case law of the CJEU, the right to access one's data may not be unduly restricted by time limits. Data subjects must also be given a reasonable opportunity to gain information about past data-processing operations.

Example: In *Rijkeboer*,[179] the CJEU was asked to determine whether, pursuant to Article 12 (a) of the directive, an individual's right of access to information on the recipients or categories of recipient of personal data and on the content of the data communicated may be limited to one year preceding his or her request for access.

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

To determine whether Article 12 (a) of the Directive authorises such a time limit, the Court decided to interpret that article in light of the purposes of the directive. The Court 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 his or her data (Article 12 (b)), or notify third parties to whom the data have been disclosed of that rectification, erasure or blocking (Article 12 (c)). The right of access is also necessary to enable the data subject to exercise his or her right to object to his personal data being processed (Article 14) or his right of action where he suffers damage (Articles 22 and 23).

In order to ensure the practical effect of the provisions referred to above, the Court 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".

The right to rectification, erasure and blocking of data

"Any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing."[180] In line with these principles, data subjects must have the right under national law to obtain from the controller the rectification, erasure or blocking of their data if they think that their processing does not comply with the provision of the directive, in particular because of the inaccurate or incomplete nature of the data.[181]

Example: In *Cemalettin Canli v. Turkey*,[182] the ECtHR found a violation of Article 8 of the ECHR in incorrect police reporting in criminal proceedings.

The applicant had twice been involved in criminal proceedings because of alleged membership in illegal organisations but was never convicted. 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 appeared as a member of two

180 Data Protection Directive, Recital 41.

181 *Ibid.*, Art. 12 (b).

182 ECtHR, *Cemalettin Canli v. Turkey*, No. 22427/04, 18 November 2008, paras. 33, 42 and 43; ECtHR, *Dalea v. France*, No. 964/07, 2 February 2010.

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 was within the scope of Article 8 of the ECHR, as public information could also fall within the scope of 'private life' where it was systematically collected and stored in files held by the authorities. Moreover, the police report was incorrect and its drafting and submission to the criminal court had not been in accordance with the law. The Court concluded that there had been a violation of Article 8.

Example: In *Segerstedt-Wiberg and Others v. Sweden*,[183] 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. The ECtHR was satisfied that the storage of the data at issue had a legal basis and pursued a legitimate aim. In respect of some of the applicants, the ECtHR found that the continued retention of the data was a disproportionate interference with their private lives. For instance, in the case of Mr Schmid, 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 not have pursued any relevant national security interest, particularly given its historical nature. The ECtHR concluded that there had been a violation of Article 8 of the ECHR in respect of four out of the five applicants.

In some cases, it will be sufficient for the data subject to simply request rectification of, for example, the spelling of a name, change of address or telephone number. If, however, such requests are linked to legal issues, 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 has been unable to challenge the accuracy of information kept in secret registers.[184]

183 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.

184 ECtHR, *Rotaru v. Romania*, No. 28341/95, 4 May 2000.

Example: In *Ciubotaru v. Moldova*,[185] 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 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. However, 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 recorded in respect of his parents by the Soviet authorities. 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.

During civil litigation or proceedings before a public authority to decide whether data are correct or not, the data subject can request that an entry or note be placed on his data file outlining that the accuracy is contested and that an official decision is pending. During this period, the data controller must not present the data as certain or final, especially to third parties.

A data subject's request to have data erased or deleted is often based on a claim that the data processing does not have a legitimate basis. Such claims often arise where consent has been withdrawn, or where certain data are no longer needed to fulfil the purpose of the data collection. The burden of proof that the data processing is legitimate will fall on the data controller, as it is responsible for the legitimacy of the processing. 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.

If the processing of data is contested because the data are allegedly incorrect or unlawfully processed, the data subject, in accordance with the principle of fair processing, can demand that the data under dispute be blocked. This means that the

185 ECtHR, *Ciubotaru v. Moldova*, No. 27138/04, 27 April 2010, paras. 51 and 59.

data are not deleted but that the controller must refrain from using the data during the period of blockage. This would be particularly necessary where continued use of inaccurate or illegitimately held data could harm the data subject. National law should provide more details about when the obligation to block the use of data may arise and how it should be exercised.

Data subjects additionally have the right to obtain from the controller the notification to third parties of any blocking, rectification or erasure, if they had received data prior to these processing operations. As the disclosure of data to third parties ought to have been documented by the controller, it should be possible to identify the data recipients and request deletion. If the data have, however, been published in the meantime, on the internet, for example, it may be impossible to have the data deleted in all instances, as the data recipients cannot be found. According to the Data Protection Directive, contacting data recipients for the rectification, deletion or blocking of data is mandatory, "unless this proves impossible or involves a disproportionate effort".[186]

5.1.2. Right to object

The right to object includes the right to object to automated individual decisions, the right to object due to the data subject's particular situation and the right to object to further use of data for direct marketing purposes.

The right to object to automated individual decisions

Automated decisions are decisions taken using personal data processed solely by automatic means. If such decisions are likely to have considerable impact on the lives of individuals as they relate, for instance, to creditworthiness, performance at work, conduct or reliability, special protection is necessary to avoid inappropriate consequences. The Data Protection Directive provides that automated decisions ought not to determine questions which are important for individuals, and requires that the individual should have the right to review the automated decision.[187]

Example: An important practical example of automated decision making is credit scoring. In order to decide quickly about the creditworthiness of a future customer, certain data such as profession and family situation are collected

186 Data Protection Directive, Art. 12 (c), last half sentence.

187 *Ibid.*, Art. 15 (1).

from the customer and combined with data about the subject available from other sources, such as credit information systems. These data are automatically fed into a scoring algorithm, which calculates an overall value representing the creditworthiness of the potential customer. Thus the company employee can decide within seconds whether the data subject is acceptable as a customer or not.

Nevertheless, according to the directive, Member States shall provide that a person may be subjected to an automated individual decision where the interests of the data subject either are not at stake, because the decision was in the data subject's favour, or are safeguarded by other appropriate means.[188] A right to object to automated decisions is also inherent in **CoE law**, as can be seen in the Profiling Recommendation.[189]

The right to object due to the data subject's particular situation

There is no general right of data subjects to object to the processing of their data.[190] Article 14 (a) of the Data Protection Directive, however, empowers the data subject to raise objection on compelling legitimate grounds relating to the data subject's particular situation. A similar right has been recognised in the CoE Profiling Recommendation.[191] Such provisions aim at finding the correct balance between the data subject's data protection rights and the legitimate rights of others in processing the data subject's data.

Example: A bank stores data for seven years on its customers who default on loan payments. A customer whose data are stored in this database applies for another loan. The database is consulted, an evaluation of the financial situation is given, and the customer is refused the loan. The customer can, however, object to having personal data recorded in the database and request the deletion of the data if he or she can prove that the payment default was merely the result of an error which had been corrected immediately after the customer had become aware of it.

188 *Ibid.*, Art. 15 (2).

189 Profiling Recommendation, Art. 5 (5).

190 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; or ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987; or ECtHR, *Mosley v. the United Kingdom*, No. 48009/08, 10 May 2011.

191 Profiling Recommendation, Art. 5 (3).

The effect of a successful objection is that the data in question may no longer be processed by the controller. Processing operations performed on the data subject's data prior to the objection, however, remain legitimate.

The right to object to further use of data for direct marketing purposes

Article 14 (b) of the Data Protection Directive provides for a specific right to object to the use of one's data for the purposes of direct marketing. Such a right is also laid down in the CoE Direct Marketing Recommendation.[192] This kind of objection is meant to be raised before data are made available to third parties for the purpose of direct marketing. The data subject must, therefore, be given the opportunity to object before the data are transferred.

5.2. Independent supervision

Key points

- In order to ensure effective data protection, independent supervisory authorities must be established under national law.
- National 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 tasks, 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 the data subject with alleged violations of data protection rights;
  - supervise controllers and processors;
  - intervene if necessary by
    - warning, admonishing or even fining controllers and processors,

192 CoE, 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).

  - ordering data to be rectified, blocked or deleted,
  - imposing a ban on processing;
- refer matters to court.

The Data Protection Directive requires independent supervision as an important mechanism to ensure effective data protection. The directive introduced an instrument for the enforcement of data protection which did not appear, at first, in Convention 108 or in the OECD Privacy Guidelines.

Given that independent supervision proved to be indispensable for the development of effective data protection, a new provision of the revised OECD Privacy Guidelines adopted in 2013 calls on Member countries to "establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis".[193]

Under CoE law, the Additional Protocol to Convention 108 has made the establishment of supervisory authorities mandatory. This instrument contains in Article 1 the legal framework for independent supervisory authorities which the Contracting Parties must implement in their domestic law. It uses similar formulations to describe the tasks and powers of these authorities as used in the Data Protection Directive. In principle, supervisory authorities should, therefore, function in the same manner under EU and CoE law.

Under EU law, the competences and organisational structure of supervisory authorities were first outlined in Article 28 (1) of the Data Protection Directive. The EU Institutions Data Protection Regulation[194] establishes the EDPS as the supervisory authority for data processing by the EU bodies and institutions. When outlining the supervisory authority's roles and responsibilities, this regulation draws on the experience gathered since the promulgation of the Data Protection Directive.

193 OECD (2013), *Guidelines governing the protection of privacy and transborder flows of personal data*, para. 19 (c).

194 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, Art. 41–48.

The independence of data protection authorities is guaranteed under Article 16 (2) of the TFEU and Article 8 (3) of the Charter. This last provision specifically views control by an independent authority as an essential element of the fundamental right to data protection. In addition, the Data Protection Directive requires Member States to establish supervisory authorities to monitor the application of the directive acting with complete independence.[195] Not only must the law underpinning a supervisory body's creation contain provisions specifically guaranteeing independence, but the specific organisational structure of the authority must demonstrate independence.

In 2010, the CJEU dealt for the first time with the question of the scope of the requirement of independence of data protection supervisory authorities.[196] The following examples illustrate its thinking.

Example: In *European Commission v. Germany*,[197] the European Commission had 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 thus failed to fulfil its obligations under Article 28 (1) of Data Protection Directive. In the Commission's view, the problem was that Germany had put under State oversight the authorities responsible for monitoring the processing of personal data outside the public sector in the different federal states (*Länder*).

The assessment of the substance of the action depended, according to the Court, on the scope of the requirement of independence contained in that provision and, therefore, on its interpretation.

The Court underlined that the words 'with complete independence' in Article 28 (1) of the directive must be interpreted based on the actual wording of that provision and on the aims and scheme of the Data Protection Directive.[198] The Court stressed that the supervisory authorities are 'the guardians' of rights related to personal data processing ensured in the directive and that their establishment in Member States is thus considered "as an essential component of the

195 Data Protection Directive, Art. 28 (1), last sentence; Convention 108, Additional Protocol, Art. 1 (3).

196 See FRA (2010), *Fundamental rights: challenges and achievements in 2010*, Annual report 2010, p. 59. The FRA addressed this issue in greater detail in its report on *Data protection in the European Union: the role of National Data Protection Authorities*, which was published in May 2010.

197 CJEU, C-518/07, *European Commission v. Federal Republic of Germany*, 9 March 2010, para. 27.

198 *Ibid*., paras. 17 and 29.

protection of individuals with regard to the processing of personal data".[199] The Court 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 of the State or the *Länder*, and not of the influence only of the supervised bodies".[200]

The CJEU also found 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. As underlined by the Court, Article 44 (2) thereof clarifies the concept of independence by adding that, in the performance of its duties, the EDPS may neither seek nor take instructions from anybody. This rules out state supervision of an independent data protection supervisory authority.[201]

Accordingly, the CJEU held that the German data protection institutions at federal state level responsible for monitoring the processing of personal data by non-public bodies were not sufficiently independent because they were subject to oversight by the state.

Example: In the *European Commission v. Austria*,[202] the CJEU highlighted similar problems concerning the position of certain members and the staff of the Austrian Data Protection Authority (Data Protection Commission, DSK). The Court concluded in this case that Austrian legislation precluded the Austrian Data Protection Authority from exercising its functions with complete independence within the meaning of the Data Protection Directive. The independence of the Austrian DPA was not sufficiently assured, because the Federal Chancellery supplies the DSK with its workforce, oversees the DSK and has the right to be informed at all times about its work.

Example: In *European Commission v. Hungary,*[203] 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".

199 *Ibid.*, para. 23.

200 *Ibid.*, para. 25.

201 *Ibid.*, para. 27.

202 CJEU, C-614/10, *European Commission v. Republic of Austria*, 16 October 2012, paras. 59 and 63.

203 CJEU, C-288/12, *European Commission v. Hungary*, 8 April 2014, paras. 50 and 67.

> The court 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 [...]."

Supervisory authorities have, under national law, powers and capabilities to:[204]

- advise controllers and data subjects on all matters of data protection;
- investigate processing operations and intervene accordingly;
- warn or admonish controllers;
- order the rectification, blocking, erasure or destruction of data;
- impose a temporary or definitive ban on processing;
- refer the 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.

There are considerable differences between domestic jurisdictions pertaining to the procedures and legal effect of a supervisory authority's findings. They can range from ombudsman-like recommendations to immediately executable decisions. Therefore, when analysing the efficiency of remedies available within a jurisdiction, the remedial instruments must be judged in their context.

5.3. Remedies and sanctions

Key points

- According to Convention 108 as well as the Data Protection Directive, national law must set out appropriate remedies and sanctions against infringements of the right to data protection.

204 Data Protection Directive, Art. 28; see further Convention 108, Additional Protocol, Art. 1.

  - The right to an effective remedy requires, under EU law that national law set out judicial remedies against infringements of data protection rights, irrespective of the possibility of approaching a supervisory authority.
  - Sanctions must be set out by national law that are effective, equivalent, proportionate and dissuasive.
- Before turning to the courts, one must first approach a controller. Whether or not it is also mandatory to approach a supervisory authority before applying to a court, is left to regulation by national law.
- Data subjects may bring violations of data protection law, as a last resort and under certain conditions, before the ECtHR.
- In addition, the CJEU can be approached by data subjects, but only to a very limited extent.

Rights under data protection law can be exercised only by the person whose rights are at stake; this will be someone who is, or at least claims to be, the data subject. Such persons may be represented in the exercise of their rights by persons who, under national law, fulfil the necessary requirements. Minors must be represented by their parents or guardians. Before the supervisory authorities, a person can also be represented by associations whose lawful aim is to promote data protection rights.

5.3.1. Requests to the controller

The rights mentioned in Section 3.2 must at first be exercised *vis-à-vis* the controller. Approaching the national supervisory authority or a court directly would not help, as the authority could only advise that the controller must be addressed first, and the court would find an application inadmissible. The formal requirements for a legally relevant request to a controller, especially whether not it must be a written request, ought to be regulated by national law.

The entity that was addressed as the controller must react to a request, even if it is not the controller. A response must, in any case, be delivered to the data subject within the timeframe set out by national law, even if it is only to say that no data are being processed about the requester. In compliance with the provisions of Article 12 (a) of the Data Protection Directive and Article 8 (b) of Convention 108, that request must be handled with 'without excessive delay'. National law should, therefore, prescribe a response period which is short enough but, nevertheless, enables the controller to deal adequately with the request.

Prior to answering the request, the entity approached as controller must establish the requester's identity to determine whether he or she is indeed the person he or she claims to be and thus avoid a serious breach of confidentiality. Where the requirements for establishing identity are not specifically regulated by national law, they must be decided by the controller. The principle of fair processing would, however, demand that controllers do not prescribe overly burdensome conditions for acknowledging identification (and the authenticity of the request, as discussed in Section 2.1.1).

National law must also deal with the question of whether or not controllers, before responding to requests, may require a fee to be paid by the requester: Article 12 (a) of the directive and Article 8 (b) of Convention 108 provide that response to access requests must be given 'without excessive [...] expense'. National law in many European countries provides that requests under data protection law must be responded to free of charge, as long as responding does not cause excessive and unusual effort; in turn, controllers are usually protected by national law against abuse of the right to obtain a response to requests.

If the person, institution or body, approached as the controller, does not deny being the controller, this entity has, within the time frame prescribed by national law, to:

- either accede to the request and notify the requesting person how the request was complied with; or
- inform the requester why his or her request will not be complied with.

5.3.2. Claims lodged with the supervisory authority

Where a person, having made a request for access or having put in an objection with a controller, does not receive an answer which is timely and satisfactory, this person can approach the national data protection supervisory authority with a claim for assistance. In the course of the proceedings before the supervisory authority, it should be clarified whether or not the person, institution or body addressed by the requester was indeed obliged to react to the request and whether the reaction was correct and sufficient. The person concerned must be informed by the supervisory authority of the outcome of the proceedings dealing with the claim.[205] The legal effects of the results of proceedings before national supervisory authorities depend

205 Data Protection Directive, Art. 28 (4).

on national law: whether the authority's decisions can be legally executed, meaning that they are enforceable by official authority, or whether it is necessary to appeal to a court if the controller does not follow the decisions (opinion, admonition, etc.) of the supervisory authority.

In the event that data protection rights guaranteed under Article 16 of the TFEU are allegedly infringed by EU institutions or bodies, the data subject may lodge a complaint with the EDPS,[206] the independent supervisory authority for data protection according to the EU Institutions Data Protection Regulation setting out the duties and powers of the EDPS. In the absence of a response from the EDPS within six months, the complaint shall be deemed to have been rejected.

Against decisions by a national supervisory authority, there must be the possibility to appeal to the courts. This applies to the data subject as well as to controllers, having been a party to proceedings before a supervisory authority.

Example: The United Kingdom Information Commissioner issued a decision on 24 July 2013 asking the Hertfordshire police to stop using a vehicle plate tracking system that it considered unlawful. The data collected by cameras were stored both in local police force databases and in a centralised database. License plate photos were stored for two years and photographs of cars for 90 days. It was held that such an extensive use of cameras and other forms of surveillance was not proportionate to the problem it was trying to address.

5.3.3. Claim lodged with a court

According to the Data Protection Directive, if the person, having made a request under data protection law to a controller, is not satisfied with the controller's response, this person must be entitled to bring a complaint before a national court.[207]

Whether or not it is mandatory to approach the supervisory authority first, before applying to a court, is left to regulation by national law. In most cases, however, it will be advantageous for the persons, exercising their data protection rights, to approach the supervisory authority first, as proceedings on claims for their

206 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.

207 Data Protection Directive, Art. 22.

assistance should be non-bureaucratic and free of charge. The expertise documented in the supervisory authority's decision (opinion, admonition, etc.) may also help the data subject to pursue his or her rights before the courts.

Under CoE law, violations of data protection rights, allegedly performed at the national level of a Contracting Party to the ECHR and constituting at the same time a violation of Article 8 of the ECHR, may, additionally, be brought before the ECtHR after exhaustion of all available domestic remedies. Pleading a violation of Article 8 of the ECHR before the ECtHR must also meet other admissibility criteria (Articles 34–37 of the ECHR).[208]

Although applications to the ECtHR can be directed only against Contracting Parties, they can also indirectly deal with actions or omissions of private parties, in so far as a Contracting Party has not fulfilled its positive obligations under the ECHR and not provided sufficient protection against infringements of data protection rights in its national law.

Example: In *K.U. v. Finland,*[209] the applicant, a minor, complained that an advertisement of a sexual nature had been posted about him on an internet dating site. The identity of the person who had posted the information was not revealed by the service provider 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, such protection was not afforded by the state, and the Court concluded that there had been a violation of Article 8 of the ECHR.

208 ECHR, Art. 34–37, available at: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

209 ECtHR, *K.U. v. Finland*, No. 2872/02, 2 December 2008.

Example: In *Köpke v. Germany,*[210] the applicant had been suspected of theft at her workplace and therefore 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 State Party has violated any of the rights protected by the ECHR, the State Party is obliged to execute the ECtHR's judgment. 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 State Party.

Under EU law,[211] the victims of infringements of national data protection law, which implements the EU data protection law, can in some cases bring their cases before the CJEU. There are two possible scenarios for how a data subject's claim that his or her data protection rights have been infringed may lead to proceedings before the CJEU.

In the first scenario, the data subject would have to be the direct victim of an EU administrative or regulatory act which violates the individual's right to data protection. According to Article 263 (4) of the TFEU:

> *"any natural or legal person may [...] institute proceedings against an act addressed to that person or which is of direct and individual concern to them, and against a regulatory act which is of direct concern to them and does not entail implementing measures."*

210 ECtHR, *Köpke v. Germany* (dec.), No. 420/07, 5 October 2010.

211 EU (2007), Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ 2007 C 306. See also the consolidated versions of the Treaty on European Union, OJ 2012 C 326 and of the TFEU, OJ 2012 C 326.

Thus, victims of the unlawful processing of their data by an EU organ can appeal directly to the CJEU's General Court, which is its body with the competence to provide judgment in matters of the EU Institutions Data Protection Regulation. The ability to apply directly to the CJEU also exists if someone's legal situation is directly affected by an EU legal provision.

The second scenario concerns the competence of the CJEU (Court of Justice) to give preliminary rulings according to Article 267 of the TFEU.

Data subjects may, in the course of domestic proceedings, ask the national court to request clarification from the Court of Justice on the interpretation of the EU Treaties and on the interpretation and validity of acts of the institutions, bodies, offices or agencies of the EU. 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.

If a party to the proceedings before the national courts requests referral of a question to the CJEU, only those national courts which act as a final resort, against whose decisions there is no judicial remedy, are obliged to comply.

Example: In *Kärntner Landesregierung and Others*,[212] the Austrian Constitutional Court submitted questions to the CJEU concerning the validity of Articles 3 to 9 of Directive 2006/24/EC (*Data Retention Directive*) in light of Articles 7, 9 and 11 of the Charter and whether or not certain provisions of the Austrian Federal Law on Telecommunications transposing the Data Retention Directive were incompatible with aspects of the Data Protection Directive and of the EU Institutions Data Protection Regulation.

Mr Seitlinger, one of the applicants in the Constitutional Court's proceedings, held that he uses the telephone, the internet and email both for work purposes and in his private life. Consequently, the information which he sends and receives passes over public telecommunication networks. Under the Austrian Telecommunications Act of 2003, his telecommunications provider is legally required to collect and store data about his use of the network. Mr Seitlinger realised that this collection and storage of his personal data was in no way necessary for the technical purposes of getting the information from A to B on the network. Nor, indeed, was the collection and storage of these data even

212 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitling and Others*, 8 April 2014.

remotely necessary for billing purposes. Mr Seitlinger had certainly not consented to this use of his personal data. The sole reason for the collection and storage of all of these extra data was 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 were breaching his fundamental rights under Article 8 of the EU Charter.

The CJEU gives a decision only on the constituent elements of the request for a preliminary ruling referred to it. The national court remains competent to decide the original case.

On principle, the Court of Justice must answer the questions put to it. It cannot refuse to give its preliminary ruling on the grounds that this response would be neither relevant nor timely as regards the original case. It can, however, refuse if the question does not fall within its sphere of competence.

Finally, if data protection rights, which are guaranteed by Article 16 of the TFEU, are allegedly infringed by an EU institution or body in the course of processing personal data, the data subject may bring the case before the General Court of the CJEU (Article 32 (1) and (4) of the EU Institutions Data Protection Regulation). The same applies to decisions of the EDPS concerning such infringements (Article 32 (3) of the EU Institutions Data Protection Regulation).

While the CJEU's General Court is competent to provide judgment in matters of the EU Institutions Data Protection Regulation, if, however, a person in the capacity of a staff member of an EU institution or body seeks a remedy, this person must appeal to the EU Civil Service Tribunal.

Example: *The European Commission v. The Bavarian Lager Co. Ltd*[213] illustrates the remedies available against activities or decisions of EU institutions and bodies relevant to data protection.

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

Bavarian Lager requested from the European Commission access to the full minutes of a meeting held by the Commission and allegedly relating to legal questions relevant to the company. The Commission had rejected the company's request for access on grounds of overriding data protection interests.[214] Against this decision, the Bavarian Lager had, in application of Article 32 of the EU Institutions Data Protection Regulation, brought a complaint before the CJEU; more precisely, before the Court of First Instance (the forerunner of the General Court). In its decision in case T-194/04, *Bavarian Lager v. Commission*, the Court of First Instance annulled the decision of the Commission to reject the access request. The European Commission appealed this decision to the Court of Justice of the CJEU. The Court of Justice gave judgment (in Grand Chamber) setting aside the judgment of the Court of First Instance and confirmed the European Commission's rejection of the request for access.

5.3.4. Sanctions

Under CoE law, Article 10 of Convention 108 provides that appropriate sanctions and remedies must be established by each Party for violations of provisions of domestic law giving effect to the basic principles of data protection set out in Convention 108.[215] **Under EU law**, Article 24 of the Data Protection Directive rules that Member States "shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted [...]".

Both instruments give Member States a wide margin of discretion in choosing the appropriate sanctions and remedies. Neither legal instrument offers particular guidance about the nature or type of appropriate sanctions, nor do they give examples of sanctions.

However:

> *"although EU Member States enjoy a margin of discretion in determining what measures are most appropriate for safeguarding rights that individuals derive from EU law, in line with the principle of loyal cooperation as laid*

214 For an analysis of the argument, see: EDPS (2011), *Public access to documents containing personal data after the* Bavarian Lager *ruling*, Brussels, EDPS, available at: www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

215 ECtHR, *I. v. Finland*, No. 20511/03, 17 July 2008; ECtHR, *K.U. v. Finland*, No. 2872/02, 2 December 2008.

down in Article 4 (3) of the TEU, the minimum requirements of effectiveness, equivalence, proportionality and dissuasiveness should be respected."[216]

The CJEU has repeatedly maintained that national law is not completely free to determine sanctions.

Example: In *Von Colson and Kamann v. Land Nordrhein-Westfalen*,[217] the CJEU pointed out that all the Member States to which a directive is addressed are obliged to adopt, in their national legal systems, all necessary measures to ensure that it is fully effective, in accordance with the objective that it pursues. The Court held that, although it is up to the Member States to choose the ways and means of ensuring that a directive is implemented, that freedom does not affect the obligation imposed on them. In particular, an effective legal remedy must enable the individual to pursue and enforce the right in question to its full substantive extent. In order to achieve that true and effective protection, legal remedies must trigger penal and/or compensatory procedures leading to sanctions with a deterrent effect.

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 are envisaged only 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 [...]".

216 FRA (2012), *Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package*, 2/2012, Vienna, 1 October 2012, p. 27.

217 CJEU, C-14/83, *Sabine von Kolson and Elisabeth Kamann v. Land Nordrhein-Westfalen*, 10 April 1984.

6 Transborder data flows

EU	Issues covered	CoE
Transborder data flows		
Data Protection Directive, Article 25 (1) CJEU, C-101/01, *Bodil Lindqvist*, 6 November 2003	Definition	Convention 108, Additional Protocol, Article 2 (1)
Free flow of data		
Data Protection Directive, Article 1 (2)	Between EU Member States	
	Between Contracting Parties to Convention 108	Convention 108, Article 12 (2)
Data Protection Directive, Article 25	To third countries with adequate level of data protection	Convention 108, Additional Protocol, Article 2 (1)
Data Protection Directive, Article 26 (1)	To third countries in specific cases	Convention 108, Additional Protocol, Article 2 (2) (a)
Restricted flow of data to third countries		
Data Protection Directive, Article 26 (2) Data Protection Directive, Article 26 (4)	Contractual clauses	Convention 108, Additional Protocol, Article 2 (2) (b) Guide to the preparation of contractual clauses
Data Protection Directive, Article 26 (2)	Binding corporate rules	
Examples: EU–US PNR-Agreement EU–US SWIFT-Agreement	Special international agreements	

The Data Protection Directive not only provides for the free flow of data between the Member States but also contains provisions on the requirements for the transfer of personal data to third countries outside the EU. The CoE also recognised the importance of implementing rules for transborder data flows to third countries and adopted the Additional Protocol to Convention 108 in 2001. This Protocol took over the main regulatory features on transborder data flows from convention parties and EU Member States.

6.1. Nature of transborder data flows

Key points

- Transborder data flow is a transfer of personal data to a recipient who or which is subject to a foreign jurisdiction.

Article 2 (1) of the Additional Protocol to Convention 108 describes transborder data flow as the transfer of personal data to a recipient who or which is subject to a foreign jurisdiction. Article 25 (1) of the Data Protection Directive regulates "transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer […]". Such data transfer is allowed only according to the rules set forth in Article 2 of the Additional Protocol to Convention 108 and, for EU Member States, additionally in Articles 25 and 26 of the Data Protection Directive.

Example: In *Bodil Lindqvist*,[218] 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 and hobbies, constitutes 'the processing of personal data wholly or partly by automatic means', within the meaning of Article 3 (1) of Directive 95/46".

The Court then pointed out that the directive also lays down specific rules intended to allow the Member States to monitor the transfer of personal data to third countries.

218 CJEU, C-101/01, *Bodil Lindqvist*, 6 November 2003, paras. 27, 68 and 69.

However, given, first, the state of development of the internet at the time the directive was drawn up and, second, the absence in the directive of criteria applicable to the use of the internet, "one cannot presume that the Community legislature intended the expression 'transfer [of data] to a third country' to cover the loading [...] of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them."

Otherwise, if the directive was "interpreted to mean that there is transfer of data to a third country every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for [by the directive] would thus necessarily become a regime of general application, as regards operations on the internet. Thus, if the Commission found [...] that even one third country did not ensure adequate protection, Member States would be obliged to prevent any personal data from being placed on the internet."

The principle that mere publication of (personal) data is not to be considered as transborder data flow applies also to online public registers or to mass media, such as (electronic) newspapers and television. Only communication which is directed at specific recipients is eligible for the concept of 'transborder data flow'.

6.2. Free data flows between Member States or between Contracting Parties

Key points

- Transfer of personal data to another member state of the European Economic Area or to another Contracting Party to Convention 108 must be free from restrictions.

According to Article 12 (2) of Convention 108, **under CoE law** there must be a free flow of personal data between the Parties to the convention. Domestic law may not restrict the export of personal data to a Contracting Party unless:

- the special nature of the data so requires;[219] or
- the restriction is necessary to avoid circumvention of domestic legal provisions on transborder data flow to third parties.[220]

Under EU law, restrictions or prohibitions on the free flow of data between Member States for reasons of data protection are forbidden by Article 1 (2) of the Data Protection Directive. The area of free data flow has been extended by the Agreement on the European Economic Area (EEA),[221] which brings Iceland, Liechtenstein and Norway into the internal market.

Example: If an affiliate of an international group of companies, being established in several EU Member States, amongst them Slovenia and France, transfers personal data from Slovenia to France, such data flow must not be restricted or prohibited by Slovenian national law.

If, however, the same Slovenian affiliate wants to transfer the same personal data to the parent company in the United States, the Slovenian data exporter must go through the proceedings laid down in Slovenian law for transborder data flow to third countries without adequate data protection, unless the parent company had joined the Safe Harbor Privacy Principles, a voluntary Code of Conduct on providing an adequate level of data protection (see Section 6.3.1).

Transborder data flows to Member States of the EEA for purposes outside the remit of the internal market, such as for investigating crimes, are not, however, subject to the provisions of the Data Protection Directive and, therefore, not covered by the principle of free flow of data. As concerns CoE law, all areas are included within the scope of Convention 108 and the Additional Protocol to Convention 108, although exemptions may be made by the Contracting Parties. All members of the EEA are also Parties to Convention 108.

219 Convention 108, Art. 12 (3) (a).

220 *Ibid.*, Art. 12 (3) (b).

221 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.

6.3. Free data flows to third countries

Key points

- Transfer of personal data to third countries shall be free from restrictions under national data protection law, if:
  - adequacy of data protection at the recipient has been ascertained; or
  - it is necessary in the specific interests of the data subject or legitimate prevailing interests of others, especially important public interests.
- Adequacy of data protection in a third country means that the main principles of data protection have been effectively implemented in the national law of this country.
- Under EU law, the adequacy of data protection in a third country is assessed by the European Commission. Under CoE law, it is left to domestic law to regulate how adequacy is assessed.

6.3.1. Free data flow because of adequate protection

CoE law permits domestic law to allow for the free flow of data to non-contracting states if the recipient state or organisation ensures an adequate level of protection for the intended data transfer.[222] Domestic law decides how to assess the level of data protection in a foreign country and who should assess it.

Under EU law, the free flow of data to third countries with an adequate level of data protection is provided for in Article 25 (1) of the Data Protection Directive. The requirement of adequacy rather than equivalence makes it possible to honour different ways of implementing data protection. According to Article 25 (6) of the directive, the European Commission is competent to assess the level of data protection in foreign countries through adequacy findings and consults on the assessment with the Article 29 Working Party which has substantially contributed to the interpretation of Articles 25 and 26.[223]

222 Convention 108, Additional Protocol, Art. 2 (1).

223 See, for example, Article 29 Working Party (2003), *Working document on transfers of personal data to third countries: applying Article 26 (2) of the EU Data Protection Directive to binding corporate rules for international data transfers*, WP 74, Brussels, 3 June 2003; and 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.

An adequacy finding by the European Commission has binding effect. If the European Commission publishes an adequacy finding for a certain country in the *Official Journal of the European Union*, all member countries of the EEA and their organs are bound to follow the decision, meaning that data can flow to this country without checking or licensing procedures before national authorities.[224]

The European Commission is also able to assess parts of a country's legal system, or confine itself to singular topics. The Commission made an adequacy finding, for instance, solely concerning Canada's private commercial legislation.[225] There are also several adequacy findings for transfers based on agreements between the EU and foreign states. These decisions refer exclusively to a single type of data transfer, such as the transmission of passenger name records by airlines to foreign border control authorities when the airline flies from the EU to certain overseas destinations (see Section 6.4.3). More recent practice of data transfer based on special agreements between the EU and third countries generally does away with the need for adequacy findings, assuming that the agreement itself offers an adequate level of data protection.[226]

One of the most important adequacy decisions does not actually relate to a set of legal provisions.[227] Rather, it concerns rules, much like a Code of Conduct, known as Safe Harbour Privacy Principles. These principles were elaborated between the EU and the US for US business companies. Membership in Safe Harbour is achieved by voluntary commitment declared before the US Commerce Department and documented in a list published by that department. As one of the important elements of adequacy is the effectiveness of the implementation of data protection, the Safe Harbour Arrangement also provides for a certain amount of state supervision: only

224 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, available at: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

225 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.

226 For instance, the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security (OJ 2012 L 215, pp. 5–14) or 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 purposes of the Terrorist Finance Tracking Program, OJ 2010 L 8, pp. 11–16.

227 European Commission (2000), 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 2000 L 215.

those companies can join the Safe Harbour, which are subject to the supervision of the US Federal Trade Commission.

6.3.2. Free data flow in specific cases

Under CoE law, Article 2 (2) of the Additional Protocol to Convention 108 allows for the transfer of personal data to third countries where there is no adequate data protection, as long as the transfer is provided for by domestic law and is necessary for the:

- specific interests of the data subject; or
- legitimate prevailing interests of others, especially important public interests.

Under EU law, Article 26 (1) of the Data Protection Directive contains provisions which are similar to those of the Additional Protocol to Convention 108.

Under the directive, interests of the data subject may justify the free flow of data to a third country if:

- the unambiguous consent of the data subject to the export of the data is given; or
- the data subject enters – or prepares to enter – into a contractual relationship which clearly requires that the data be transferred to a recipient abroad; or
- a contract between a data controller and a third party was closed in the interests of the data subject; or
- transfer is necessary in order to protect the vital interests of the data subject.
- for the transfer of data from public registers; this is an instance of prevailing interests in the general public to be able to access information stored in public registers.

The legitimate interests of others may justify free transborder flow of data:[228]

228 Data Protection Directive, Art. 26 (1) (d).

- owing to an important public interest, other than matters of national or public security, as they are not covered by the Data Protection Directive; or

- to establish, exercise or defend legal claims.

The cases referred to above must be understood as exemptions from the rule that uninhibited data transfer to other countries requires an adequate level of data protection in the recipient country. Exemptions must always be interpreted restrictively. This has been underlined repeatedly by the Article 29 Working Party in the context of Article 26 (1) of the Data Protection Directive, particularly if consent is the purported basis for data transfer.[229] The Article 29 Working Party has concluded that the general rules on the legal significance of consent also apply to Article 26 (1) of the directive. If, in the context of labour relations, for example, it is unclear that the consent given by employees was actually free consent, then data transfers cannot be founded on Article 26 (1) (a) of the directive. In such cases, Article 26 (2), which requires national data protection authorities to issue a licence for data transfers, will apply.

6.4. Restricted data flows to third countries

Key points

- Before exporting data to third countries not ensuring an adequate level of data protection, the controller may be required to subject the intended data flow to examination by the supervisory authority.
- The controller who wants to export data must demonstrate two issues during this examination:
  - that a legal basis exists for the data transfer to the recipient; and
  - that measures are in place to safeguard adequate protection of the data at the recipient.
- Measures for establishing adequate data protection at the recipient may include:
  - contractual stipulations between the data-exporting controller and the foreign data recipient; or

229 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.

  - binding corporate rules, usually applicable for data transfers within a multinational group of companies.
- Data transfers to foreign authorities can also be governed by a special international agreement.

The Data Protection Directive and the Additional Protocol to Convention 108 permit domestic law to establish regimes for transborder data flows to third countries not ensuring an adequate level of data protection, so long as the controller has made special arrangements to ensure adequate data protection safeguards at the recipient and so long as the controller can prove this to a competent authority. This requirement is explicitly mentioned only in the Additional Protocol to Convention 108; however, it is also considered to be standard procedure under the Data Protection Directive.

6.4.1. Contractual clauses

Both **CoE law** and **EU law** mention contractual clauses between the data-exporting controller and the recipient in the third country as a possible means of safeguarding a sufficient level of data protection at the recipient.

At the **EU level**, the European Commission with the assistance of the Article 29 Working Party developed standard contractual clauses which were officially certified by a Commission Decision as proof of adequate data protection.[230] As Commission decisions are binding in their entirety in the Member States, the national authorities in charge of supervising transborder data flows must acknowledge these standard contractual clauses in their procedures.[231] 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.

The existence of standard contractual clauses in the EU legal framework does not prohibit controllers from formulating other *ad hoc* contractual clauses. They would, however, have to produce the same level of protection as provided by the standard contractual clauses. The most important features of the standard contractual clauses are:

230 Data Protection Directive, Art. 26 (4).

231 TFEU, Art. 288.

- 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 procedure of the data-exporting controller's national supervisory authority and/or courts in case of dispute.

There are now two sets of standard clauses for controller-to-controller transfers available, from which the data-exporting controller can choose.[232] For controller-to-processor transfers, there is only one set of standard contractual clauses.[233]

Within the context of **CoE law**, the Consultative Committee of Convention 108 drew up a guide on the preparation of contractual clauses.[234]

6.4.2. Binding corporate rules

Multilateral binding corporate rules (BCRs) very often involve several European data protection authorities at the same time.[235] In order for BCRs to be approved, the draft of the BCRs must be sent together with the standardised application forms to the lead authority.[236] The lead authority is identifiable from the standardised application form. This authority then informs all of the supervisory authorities in EEA member countries where affiliates of the group are established, although their participation in the evaluation process of the BCRs is voluntary. Although it is not binding, all

232 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.

233 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.

234 CoE, Consultative Committee of the Convention 108 (2002), *Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data*.

235 The content and structure of appropriate binding corporate rules are explained in Article 29 Working Party (2008), *Working document setting up a framework for the structure of Binding Corporate Rules*, WP 154, Brussels, 24 June 2008; and in Article 29 Working Party (2008), *Working document setting up a table with the elements and principles to be found in Binding Corporate Rules*, WP 153, Brussels, 24 June 2008.

236 Article 29 Working Party (2007), *Recommendation 1/2007 on the standard application for approval of binding corporate rules for the transfer of personal data*, WP 133, Brussels, 10 January 2007.

data protection authorities concerned should incorporate the result of the evaluation into their formal licensing procedures.

6.4.3. Special international agreements

The EU has concluded special agreements for two types of data transfers:

Passenger Name Records

Passenger Name Records (PNR) data are collected by air carriers during the reservation process and include names, addresses, credit card details and seat numbers of air passengers. Under United States (US) law, air carrier companies are obliged to make these data available to the Department of Homeland Security prior to passenger departure. This applies to flights to or from the US.

To ensure adequate protection of PNR data in accordance with the provisions of Directive 95/46/EC, a 'PNR package'[237] was adopted in 2004. The package included the adequacy of the data processing carried out by the US Department of Homeland Security (DHS).

Following the CJEU's annulment of the PNR package,[238] the EU and the United States signed two separate agreements with a twofold purpose: first, to provide a legal basis for the disclosure of PNR data to the US authorities, and second, to establish adequate data protection in the recipient country.

The first agreement on how EU countries and the United States share and manage data, signed in 2012, had several flaws and was replaced in the same year with another agreement to ensure better legal certainty.[239] The new agreement offers

237 Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, OJ 2004 L 183, p. 83, and Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection, OJ 2004 L 235, pp. 11-22.

238 CJEU, Joined cases C-317/04 and C-318/04, *European Parliament v. Council of the European Union*, 30 May 2006, paras. 57, 58 and 59, in which the Court ruled that both the adequacy decision and the agreement relating to the processing of data are excluded from the scope of Directive.

239 Council Decision 2012/472/EU of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ 2012 L 215/4. The Agreement's text is attached to this Decision, OJ 2012 L 215, pp. 5-14.

significant improvements. It restricts and clarifies the purposes for which the information may be used, such as serious transnational crimes and terrorism, and it establishes the time period for which data may be retained: after six months, the data must be depersonalised and masked. Should their data be misused, everyone has the right to administrative and judicial redress in accordance with US law. They also have the right to access their own PNR data and seek rectification by the US Department of Homeland Security, including the possibility of erasure, if the information is inaccurate.

The agreement, which entered into force on 1 July 2012, shall remain in force for seven years, until 2019.

In December 2011, the Council of the European Union approved the conclusion of an updated EU-Australia Agreement on the processing and transfer of PNR data.[240] The agreement between the EU and Australia on PNR data is a further step in the EU agenda, which includes global PNR guidelines,[241] setting up an EU-PNR scheme[242] and negotiating agreements with third countries.[243]

Financial messaging data

The Belgian-based Society for Worldwide Interbank Financial Telecommunication (SWIFT), which is the processor for most of the global money transfers from European banks, was operating with a mirror centre in the US and was confronted

240 Council Decision 2012/381/EU of 13 December 2011 on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, OJ 2012 L 186/3. The text of the Agreement, which replaced a previous 2008 agreement, is attached to this Decision, OJ 2012 L 186, pp. 4–16.

241 See in particular the Communication of the Commission of 21 September 2010 on the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM(2010) 492 final, Brussels, 21 September 2010. See also Article 29 Working Group (2010), *Opinion 7/2010 on the European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries*, WP 178, Brussels November 12, 2010.

242 Proposal for a Directive of the European Parliament and of the Council on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, Brussels, 2 February 2011. In April 2011, the European Parliament requested FRA to provide an opinion on this Proposal and its compliance with the Charter of Fundamental Rights of the European Union. See: FRA (2011), *Opinion 1/2011 – Passenger Name Record*, Vienna, 14 June 2011.

243 The EU is negotiating a new PNR agreement with Canada, which will replace the 2006 agreement currently in force.

with the request to disclose data to the US Department of the Treasury for terrorism investigation purposes.[244]

From the EU perspective, there was no sufficient legal basis for disclosing these substantially European data, which were accessible in the United States only because one of SWIFT's data service-processing centres was located there.

A special agreement between the EU and the United States, known as the SWIFT Agreement, was concluded in 2010 to provide the necessary legal basis and to secure adequate data protection.[245]

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).

Europol must receive a copy of each request by the US Treasury Department and verify whether or not the principles of the SWIFT Agreement are complied with.[246] If it is confirmed that they are, SWIFT must provide the financial data directly to the

244 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.

245 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.

246 The Joint Supervisory Body of Europol has conducted audits on Europol's activities in this area, the results of which are available at: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

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 shall be deleted no later than five years from receipt. Financial data which are relevant for specific investigations or prosecutions may be retained 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 United States 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.

Data subjects have a right to obtain confirmation from the competent EU data protection authority that their personal data protection rights have been complied with. Data subjects also have the right to rectification, erasure or blocking of their data 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 their right to seek administrative and judicial redress in the United States.

The SWIFT Agreement is valid for five years, 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.

7

Data protection in the context of police and criminal justice

EU	Issues covered	CoE
	In general	Convention 108
	Police	Police Recommendation
		ECtHR, *B.B. v. France*, No. 5335/06, 17 December 2009
		ECtHR, *S. and Marper v. the United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008
		ECtHR, *Vetter v. France*, No.59842/00, 31 May 2005
	Cybercrime	Cybercrime Convention
Data protection in the context of cross-border cooperation of police and judicial authorities		
Data Protection Framework Decision	In general	Convention 108
		Police Recommendation
Prüm Decision	For special data: fingerprints, DNA, hooliganism etc.	Convention 108
		Police Recommendation
Europol Decision	By special agencies	Convention 108
Eurojust Decision		Police Recommendation
Frontex Regulation		
Schengen II Decision	By special joint information systems	Convention 108
VIS Regulation		Police Recommendation
Eurodac Regulation		ECtHR, *Dalea v. France*, No. 964/07, 2 February 2010
CIS Decision		

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.

7.1. CoE law on data protection in police and criminal justice matters

Key points

- Convention 108 and the CoE Police Recommendation cover 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.

At the European level, Convention 108 covers all fields of processing personal data, and its provisions are intended to regulate the processing of personal data in general. Consequently, Convention 108 applies to data protection in the area of police and criminal justice although the Contracting Parties may limit its application.

The legal tasks of police and criminal justice authorities often require the processing of personal data which may entail serious consequences for the individuals concerned. The Police Data Recommendation adopted by the CoE in 1987 gives guidance to the Contracting Parties on how they should give effect to the principles of Convention 108 in the context of personal data processing by police authorities.[247]

7.1.1. 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 interferences.[248]

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

248 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.

Example: In *B.B. v. France*,[249] the ECtHR decided that the inclusion of 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 right of the data subject to request erasure of the data, the limited length of data storage and the limited 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*,[250] both applicants had been charged with, but not convicted of, criminal offences. Nonetheless, their fingerprints, DNA profiles and cellular samples were kept and stored by the police. The unlimited retention of 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.

Many further ECtHR judgments deal with the justification of interference with the right to data protection by surveillance.

Example: In *Allan v. the United Kingdom,*[251] private conversations of a prisoner with a friend in the prison visiting area and with a co-accused in a prison cell were secretly recorded by the authorities. 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, the said interference was not in accordance with the law. The Court concluded that there had been a violation of Article 8 of the ECHR.

249 ECtHR, *B.B. v. France*, No. 5335/06, 17 December 2009.

250 ECtHR, *S. and Marper v. the United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008, paras. 119 and 125.

251 ECtHR, *Allan v. the United Kingdom*, No. 48539/99, 5 November 2002.

Example: In *Klass and Others v. Germany*,[252] the applicants claimed that several German legislative acts allowing secret surveillance of mail, post and telecommunication violated Article 8 of the ECHR, notably because the person concerned was not informed of the surveillance measures and could not have recourse to the courts once such measures were terminated. The ECtHR held that a threat of surveillance necessarily interfered with freedom of communication between users of the postal and telecommunication services. However, it found that sufficient safeguards against abuse had been put in place. The German legislature was justified in considering such measures necessary in a democratic society in the interests of national security and for the prevention of disorder or crime. The Court concluded that there had not 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 keeping databases in this area are especially necessary. The CoE Police Recommendation sought to address the issue by giving guidance on how data should be collected for police work; how data files in this area should be kept; who should be allowed access to these files, including the conditions for transferring 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 is also considered.

The recommendation does not provide for an open-ended, indiscriminate collection of 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 suppression 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 absolute necessity in the context of a particular inquiry.

Where personal data are collected without the knowledge of the data subject, the data subject ought to be informed of the data collection as soon as such disclosure no longer inhibits investigations. The collection of data by technical surveillance or other automated means should also be based on specific legal provisions.

252 ECtHR, *Klass and Others v. Germany*, No. 5029/71, 6 September 1978.

Example: In *Vetter v. France*,[253] anonymous witnesses had accused the applicant of homicide. As the applicant regularly went to a friend's home, the police installed listening devices there with the permission of the investigating judge. On the strength of the conversations that were recorded, the applicant was arrested and prosecuted for homicide. He applied to have the recording declared inadmissible in evidence, arguing in particular that it had not been provided for by law. For the ECtHR, the point at issue was whether or not the use of listening devices was "in accordance with the law". The bugging of private premises was manifestly not within the scope of Articles 100 *et seq.* of the Code of Criminal Procedure, since those provisions concerned the interception of telephone lines. Article 81 of the Code did not indicate with reasonable clarity the scope or manner of exercise of the authorities' discretion in allowing the monitoring of private conversations. Accordingly, the applicant had not enjoyed the minimum degree of protection to which citizens were entitled under the rule of law in a democratic society. The Court concluded that there had been a violation of Article 8 of the ECHR.

The recommendation concludes that, when storing personal data, clear distinctions should be made between: administrative data and police data; 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.

Police data should be strictly limited in purpose. This has consequences for the communication of police data to third parties: the transfer or communication 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 communication of such data outside the police sector should be allowed only where there is a clear legal obligation or authorisation. International transfer or communication 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 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, the data subject must have the right under domestic

253 ECtHR, *Vetter v. France*, No. 59842/00, 31 May 2005.

law to appeal to the national data protection supervisory authority or to another independent body.

7.1.2. 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.[254] This convention is open for accession also by non-members of the CoE and, by mid-2013, four states outside the CoE – Australia, the Dominican Republic, Japan and the United States – were parties to the convention and 12 other non-members had signed it or 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 actually an instrument for promoting data protection, it criminalises activities which are likely to violate a data subject's right to the protection of his or her data. It also obliges the Contracting Parties when implementing the convention to foresee adequate protection of human rights and liberties, including rights guaranteed under the ECHR, such as the right to data protection.[255]

254 Council of Europe, Committee of Ministers (2001), Convention on Cybercrime, CETS No. 185, Budapest, 23 November 2001, entered into force on 1 July 2004.

255 *Ibid.*, Art. 15 (1).

7.2. EU law on data protection in police and criminal matters

Key points

- At the EU level, data protection in the police and criminal justice sector is regulated only in the context of cross-border cooperation of police and judicial authorities.
- Special data protection regimes exist for the European Police Office (Europol) and the EU Judicial cooperation unit (Eurojust), which are EU bodies assisting and promoting cross-border law enforcement.
- Special data protection regimes also exist for the joint information systems which are established at the EU level for cross-border information exchange between the competent police and judicial authorities. Important examples are Schengen II, the Visa Information System (VIS) and Eurodac, a centralised system containing the fingerprint data of third-country nations applying for asylum in one of the EU Member States.

The Data Protection Directive does not apply to the area of police and criminal justice. Section 7.2.1 describes the most important legal instruments in this field.

7.2.1. The Data Protection Framework Decision

The Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (*Data Protection Framework Decision*)[256] aims at providing protection of personal data of natural persons when their personal data are processed for the purpose of preventing, investigating, detecting or prosecuting a criminal offence or of executing a criminal penalty. Acting on behalf of the Member States or the EU are competent authorities working in the area of police and criminal justice. These authorities are EU agencies or bodies, as well as authorities of the Member States.[257] The applicability of the framework decision is limited to ensuring data protection in the cross-border cooperation between these authorities and does not extend to national security.

256 Council of the European Union (2008), Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (*Data Protection Framework Decision*), OJ 2008 L 350.

257 *Ibid.*, Art. 2 (h).

The Data Protection Framework Decision relies to a large extent on the principles and definitions which are contained in Convention 108 and in the Data Protection Directive.

Data must be used only by a competent authority and only for the purpose for which they were transmitted or made available. The receiving Member State must respect any restrictions on the exchange of data provided for in the law of the transmitting Member State. Use of data by the recipient state for a different purpose is, however, allowed under certain conditions. The logging and documenting of transmissions is a specific duty of the competent authorities in order to assist with the clarification of responsibilities arising from complaints. Onward transfer of data, received in the course of cross-border cooperation, to third parties requires the consent of the Member State from which the data originate, although there are exemptions in urgent cases.

The competent authorities must take the necessary security measures to protect personal data against any unlawful form of processing.

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 Data Protection Framework Decision. They 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.

The data subject is entitled to information about the processing of his or her personal data, and has the right of access, rectification, erasure or blocking. Where the exercise of these 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 violations of the national law implementing the Data Protection Framework Decision, this person is entitled to compensation from the controller.[258] Generally, data subjects must have access to a judicial remedy for any breach of their rights guaranteed by national law implementing the Data Protection Framework Decision.[259]

258 *Ibid.*, Art. 19.

259 *Ibid.*, Art. 20.

The European Commission proposed a reform, which consists of a General Data Protection Regulation,[260] and a General Data Protection Directive.[261] This new Directive will replace the current Data Protection Framework Decision and apply general principles and rules to police and judicial cooperation in criminal matters.

7.2.2. More specific legal instruments on data protection in police and law-enforcement cross-border cooperation

In addition to the Data Protection Framework Decision, 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 and the Council Decision concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information.[262]

Importantly, cross-border cooperation[263] between the competent authorities increasingly involves the exchange of immigration data. This area of law does not belong to 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 EU has heightened the risk of fraud, making it necessary for Member States to intensify cooperation, notably by enhancing cross-border information

260 European Commission (2012), *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012) 11 final, Brussels, 25 January 2012.

261 European Commission (2012), *Proposal for 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 the free movement of such data (General Data Protection Directive)*, COM(2012) 10 final, Brussels, 25 January 2012.

262 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.

263 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.

exchange, to more effectively detect and prosecute violations of national and EU customs law.

The Prüm Decision

An important example of institutionalised cross-border cooperation by exchange of nationally held data is Council 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.[264] The Prüm Treaty was an international police cooperation agreement signed in 2005 by Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Spain.[265]

The aim of the Prüm Decision is to help 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 in order to prevent terrorist offences;
- other measures for stepping up cross-border police cooperation.

The databases which are made available under the Prüm Decision are governed entirely by national law, but the exchange of data is additionally governed by the decision and, more recently, the Data Protection Framework Decision. The competent bodies for supervision of such data flows are the national data protection supervisory authorities.

264 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.

265 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; available at: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

7.2.3. Data protection at Europol and Eurojust

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 Council Decision establishing the European Police Office (*Europol Decision*).[266] 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 the Annex of the Europol Decision, which affect two or more Member States.

In order 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 from it. Only the party which entered the data into the system may modify, correct or delete them.

Where necessary for the performance of its tasks, Europol may store, modify and use data concerning criminal offences in analysis work files. Analysis work files are opened for the purpose of assembling, processing or using data with the aim of assisting concrete criminal investigations which are conducted by Europol together with EU Member States.

In response to new developments, the European Cybercrime Centre was established at Europol on 1 January 2013.[267] The centre serves as the EU information hub on cybercrime, contributing to faster reactions in the event of online crimes, developing

266 Council of the European Union (2009), Council Decision of 6 April 2009 establishing the European Police Office, OJ 2009 L 121 (Europol). See also the Commission's proposal for a regulation therefore provides for a legal framework for a new Europol which succeeds and replaces Europol as established by the Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), and CEPOL as established by Council Decision 2005/681/JHA establishing the European Police College (CEPOL), COM(2013) 173 final.

267 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.

and deploying digital forensic capabilities and delivering best practice on cybercrime investigations. The centre focuses on cybercrime which:

- 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 and information systems in the EU.

The data protection regime governing Europol's activities is enhanced. The Europol Decision states in its Article 27 that the principles, which are set out in Convention 108 and in the Police Data Recommendation regarding the processing of automated and non-automated data, apply. Data transmission between Europol and the Member States must also satisfy the rules contained in the Data Protection Framework Decision.

To ensure compliance with applicable data protection law and, in particular, that the rights of the individual are not violated by the processing of personal data, the independent Europol Joint Supervisory Body (JSB) reviews and monitors the activities of Europol.[268] 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. If a person is not satisfied with Europol's decision regarding the exercise of these rights, he or she may appeal to the JSB Appeals Committee.

If damage occurred as a result of legal or factual errors in data stored or processed at Europol, the injured party may seek redress only before the competent court of the Member State in which the event causing the damage occurred.[269] Europol will reimburse the Member State if the damage is the result of a failure by Europol to comply with its legal obligations.

268 Europol Decision, Art. 34.

269 *Ibid.*, Art. 52.

Eurojust

Eurojust, set up in 2002, is an EU body, headquartered in The Hague, that promotes judicial cooperation in investigations and prosecutions relating to serious crime concerning at least two Member States.[270] 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 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 it 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.[271] 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 the Council of Europe Convention 108 and its

270 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*).

271 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).

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.[272]

An independent 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 reply 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.

7.2.4. Data protection in the joint information systems at EU level

In addition to data exchange between Member States and the creation of specialised EU authorities for fighting transborder crime, several joint information systems have been established at the EU level to serve as a platform for data exchange between the competent national and EU authorities for specified purposes of law enforcement, including immigration law and customs law. Some of these systems developed out of multilateral agreements which were subsequently supplemented by EU legal instruments and systems, such as the Schengen Information System, Visa Information System, Eurodac, Eurosur or Customs Information System.

The European Agency for Large-scale information technology systems (eu-LISA),[273] established in 2012, is responsible for the long-term operational management of the second-generation Schengen Information System (SIS II), the Visa Information System (VIS) 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.

272 Rules of Procedure on the Processing and Protection of Personal Data at Eurojust, OJ 2005 C 68/01, 19 March 2005, p. 1.

273 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.

The Schengen Information System

In 1985, several Member States of the former European Communities 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.[274] In order to counterbalance the threat to public security which 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.[275] 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 all EU Member States plus Iceland, Liechtenstein, Norway and Switzerland.[276] 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. C-SIS is used by national border control, police, customs, visa 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. The N-SIS is consulted and will issue an alert where:

- 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; or

274 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.

275 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.

276 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.

- 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.

In case of an alert, follow-up activities are to be initiated via the National Schengen Information Systems.

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; and enhanced alerts on persons and objects; copies of European Arrest Warrants (EAWs) on persons wanted for arrest, surrender or extradition.

Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System (Schengen II Decision) incorporates Convention 108: "Personal data processed in application of this decision shall be protected in accordance with the Council of Europe Convention 108".[277] Where the use of personal data by national police authorities is done in application of the Schengen II Decision, the provisions of Convention 108, as well as of the Police Data Recommendation, must be implemented in national law.

The competent national supervisory authority in each Member State supervises the domestic N-SIS. In particular, it must check on the quality of the data which the Member State enters into C-SIS via the 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. The national supervisory authorities and the EDPS cooperate and ensure coordinated supervision of the 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.

Access rights of individuals concerning the SIS II may be exercised in any Member State, as every N-SIS is a precise copy of the C-SIS.

277 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, OJ 2007 L 205, Art. 57.

Example: In *Dalea v. France*,[278] 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 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.[279] The VIS allows Schengen states to exchange visa data through a system which connects the consulates 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 to transit through the Schengen area. The VIS enables border authorities to verify, with the help of biometric data, whether or not the person presenting a visa is its rightful holder and to identify persons with no or fraudulent documents.

According to 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*), only data on the applicant, his or her visas, photographs, fingerprints, links to previous applications, and

278 ECtHR, *Dalea v. France* (dec.), No. 964/07, 2 February 2010.

279 Council of the European Union (2004), Council Decision 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.

application files of persons accompanying him or her, may be recorded in the VIS.[280] Access to the VIS in order to enter, amend or delete data is restricted exclusively to the visa authorities of the Member States, whereas access for 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, national competent police authorities and Europol may request access to data entered into the VIS for the purpose of preventing, detecting and investigating terrorist and criminal offences.[281]

Eurodac

Eurodac's name refers to dactylograms, or fingerprints. It is a centralised system containing the fingerprint data of third-country nationals applying for asylum in one of the EU Member States.[282] The system has been in operation since January 2003, and its purpose is to assist in determining which Member State should be responsible for examining a particular asylum application under Council Regulation (EC) No. 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national (*Dublin II Regulation*).[283] Personal data in Eurodac may be used only for the purpose of facilitating the application of the Dublin II Regulation; any other use is subject to penalties.

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 non-EU national or stateless person of at least 14 years of age who asks

280 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.

281 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.

282 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*).

283 Council Regulation (EC) No. 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, OJ 2003 L 50 (*Dublin II Regulation*).

for asylum in their territory, or 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 found staying within their territory without permission.

The fingerprint data are stored in the Eurodac database only in pseudonymised form. In the event of a match, the pseudonym, together with the name of the first Member State which transmitted the fingerprint data, is disclosed to the second Member State. This second Member State will then approach the first Member State because, according to the Dublin II Regulation, the first Member State is responsible for processing the asylum application.

Personal data stored in Eurodac which 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 two years. These data must be erased immediately if the data subject receives a residence permit, leaves EU territory or obtains citizenship of a Member State.

In addition to all EU Member States, Iceland, Norway, Liechtenstein and Switzerland also apply Eurodac on the basis of international agreements.

Eurosur

The European Border Surveillance System (*Eurosur*)[284] is designed to enhance the control of the Schengen external borders by detecting, preventing and combating illegal 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.[285] Its general objectives are:

- to reduce the number of illegal migrants entering the EU undetected;

284 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.

285 Regulation (EU) No. 1168/2011 of the European Parliament and of the Council of 25 October 2011 amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ 2011 L 394 (*Frontex Regulation*).

- to reduce the number of deaths of illegal 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.[286]

It took up its work on 2 December 2013 in all member states with external borders, and will begin from 1 December 2014 in the others. The regulation will apply to the surveillance of land, sea external borders and air borders of the Member States.

Customs Information System

Another important joint information system established at EU level is the Customs Information System (CIS).[287] 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 information contained in CIS comprises personal data with reference to commodities, means of transport, businesses, persons, goods and cash retained, seized or confiscated. 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.

286 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.

287 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*).

The processing of personal data must comply with the specific rules established by Regulation No. 515/97 and the CIS Convention,[288] as well as the provisions of the Data Protection Directive, the EU Institutions Data Protection Regulation, Convention 108 and the Police Data Recommendation. The EDPS is responsible for the supervision of compliance of the CIS with Regulation (EC) No. 45/2001 and convenes a meeting at least once a year with all national data protection supervisory authorities competent for CIS-related supervisory issues.

288 *Ibid.*

8 Other specific European data protection laws

EU	Issues covered	CoE
Data Protection Directive Directive on privacy and electronic communications	Electronic communications	Convention 108 Telecommunication Services Recommendation
Data Protection Directive, Article 8 (2) (b)	Employment relations	Convention 108 Employment Recommendation
		ECtHR, *Copland v. the United Kingdom*, No. 62617/00, 3 April 2007
Data Protection Directive, Article 8 (3)	Medical data	Convention 108 Medical Data Recommendation
		ECtHR, *Z. v. Finland*, No. 22009/93, 25 February 1997
Clinical Trials Directive	Clinical trials	
Data Protection Directive, Article 6 (1) (b) and (e), Article 13 (2)	Statistics	Convention 108 Statistical Data Recommendation
Regulation (EC) No. 223/2009 on European statistics CJEU, C-524/06, *Huber v. Germany*, 16 December 2008	Official statistics	Convention 108 Statistical Data Recommendation

Directive 2004/39/EC 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**	Convention 108 Recommendation 90(19) used for payments and other related operations ECtHR, *Michaud v. France*, No. 12323/11, 6 December 2012

In several instances, special legal instruments have been adopted at the European level, which apply the general rules of Convention 108 or of the Data Protection Directive in more detail to specific situations.

8.1. Electronic communications

Key points

- Specific rules on data protection in the area of telecommunication, with particular reference to telephone services, are contained in the CoE Recommendation from 1995.
- 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 pertains not only to the content of a communication but also to traffic data, such as information about who communicated with whom, when and for how long, and location data, such as from where data were communicated.

Communications networks have a heightened potential for unjustified interference with the personal sphere of the users, as they provide added technical possibilities for listening into and surveying communications performed on such networks. Consequently, special data protection regulations were deemed necessary in order to meet the particular risks for users of communications services.

In 1995, the CoE issued a Recommendation for data protection in the area of telecommunication, with particular reference to telephone services.[289] According to

289 CoE, 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.

this recommendation, the purposes of collecting and processing personal data in the context of telecommunications should be limited to: connecting a user to the network, making available the particular telecommunications service, billing, verifying, ensuring optimal technical operation and developing the network and service.

Special attention was given also 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 advertising messages. 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.

As concerns 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, with the purpose of complementing and particularising the provisions of the Data Protection Directive for the telecommunications sector.[290] 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 traffic data, such as information about the communication partners, time and duration of the communication;

- within the traffic data, there are data specifically relating to the location of the communication device, so-called location data; these data are at the same time

290 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 and particularly relevant concerning users of mobile communication devices.

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 on the next metro station or pharmacy or the weather forecast for this location.

Other access to data about communications in electronic networks, such as access for the purpose of investigating crimes, must, according to Article 15 of the e-Privacy Directive, fulfil the requirements for justified interference into the right to data protection as laid down in Article 8 (2) of the ECHR and confirmed by the Charter in its Articles 8 and 52.

The amendments from 2009 to the Directive on privacy and electronic communications[291] 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.[292]

- Setting of cookies, software which monitors and records a computer user's actions, is no longer allowed without the computer user's consent. National law should regulate in more detail how consent should be expressed and obtained in order to offer sufficient protection.[293]

291 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.

292 See the amended Directive, Art. 13.

293 See *Ibid.,* Art. 5; see also Article 29 Working Party (2012), *Opinion 04/2012 on cookie consent exemption*, WP 194, Brussels, 7 June 2012.

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.[294]

The Data Retention Directive[295] (invalidated on 8 April 2014, see case example below) obliged communication service providers to keep traffic data available, specifically for the purposes of fighting serious crime, for a period of at least six but not more than 24 months, regardless of whether or not the provider still needed these data for billing purposes or to technically provide the service.

The EU Member States shall designate independent public authorities which are responsible for monitoring the security of the retained data.

The retention of telecommunications data clearly interferes with the right to data protection.[296] Whether or not this interference is justified has been contested in several court procedures in EU Member States.[297]

> Example: In *Digital Rights Ireland and Seitlinger and Others,*[298] the CJEU declared the Data Retention Directive to be invalid. According to the Court, "the wide-ranging and particularly serious interference of the directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary."

A crucial issue in the context of electronic communications is interference by public authorities. Means of surveillance or interception of communications, such as

294 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.

295 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.

296 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.

297 Germany, Federal Constitutional Court (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 March 2010; Romania, Federal Constitutional Court (*Curtea Constituţională a României*), No. 1258, 8 October 2009; the Czech Republic, Constitutional Court (*Ústavní soud České republiky*), 94/2011 Coll., 22 March 2011.

298 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others,* 8 April 2014, para. 65.

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 interest of: protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences; or protecting the data subject or the rights and freedoms of others.

Example: In *Malone v. the United Kingdom,*[299] the applicant had been charged with a number of offences relating to dishonest handling of stolen goods. During his trial it emerged that a telephone conversation of the applicant had been intercepted on the authority of a warrant issued by the Secretary of State for the Home Department. Even though the manner in which the applicant's communication had been intercepted was lawful in terms of domestic law, the ECtHR found that there had been no legal rules concerning the scope and manner of exercise of the discretion enjoyed by the public authorities in this area and that the interference resulting from the existence of the practice in question had therefore not been 'in accordance with the law'. The Court held that there had been a violation of Article 8 of the ECHR.

8.2. Employment data

Key points

- Specific rules for data protection in employment relations are contained in the CoE Employment Data Recommendation.
- In the Data Protection Directive, 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 doubtful, considering the economic imbalance between employer and employees. The circumstances of consenting must be assessed carefully.

There is no specific legal framework in the EU governing data processing in the context of employment. In the Data Protection Directive, employment relations are specifically referred to only in Article 8 (2) of the directive, which concerns the

299 ECtHR, *Malone v. the United Kingdom*, No. 8691/79, 2 August 1984.

processing of sensitive data. As regards the CoE, the Employment Data Recommendation was issued in 1989 and is currently being updated.[300]

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.[301] The working party analysed the significance of consent as a legal basis for processing employment data.[302] The working party found that the economic imbalance between the employer asking for consent and the employee giving consent will often raise doubts about whether consent was given freely or not. The circumstances under which consent is requested 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 legitimate extent of monitoring employees' electronic communications 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 following ECtHR judgment is of particular interest in this context:

> Example: In *Copland v. UK*,[303] the telephone, email and internet usage of a college employee was secretly monitored in order 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

300 Council of Europe, Committee of Ministers (1989), Recommendation Rec(89)2 to member states on the protection of personal data used for employment purposes, 18 January 1989. See further Consultative Committee to Convention 108, Study on Recommendation No. R (89) 2 on the protection of personal data used for employment purposes and to suggest proposals for the revision of the above-mentioned Recommendation, 9 September 2011.

301 Article 29 Working Party (2001), *Opinion 8/2001 on the processing of personal data in the employment context*, WP 48, Brussels, 13 September 2001.

302 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.

303 ECtHR, *Copland v. the United Kingdom*, No. 62617/00, 3 April 2007.

interference was not in accordance with the law. The Court concluded that there had been a violation of Article 8 of the ECHR.

According to the CoE Employment Recommendation, personal data collected for employment purposes should be obtained from the individual employee directly.

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 in so far as this is necessary to allow them to represent the interests of the employees.

Sensitive personal data collected for employment purposes may only be processed in particular cases and according to the safeguards laid down by domestic law. Employers may ask employees or job applicants about their state of health or may examine them medically only if necessary to: determine their suitability for the employment; fulfil the requirements of preventative medicine; or allow social benefits to be granted. 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 it.

Under the Employment Recommendation, employees should be informed about the purpose of the processing of their personal data, the type of personal data stored, the entities to which the data are regularly communicated and the purpose and legal basis of such communications. Employers should also inform their employees in advance about the introduction or adaptation of automated systems for the processing of personal data of employees or for monitoring the movements or the productivity of employees.

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.

8.3. Medical data

Key point

- Medical data are sensitive data and, therefore, enjoy specific protection.

Personal data concerning the state of health of the data subject are qualified as sensitive data under Article 8 (1) of the Data Protection Directive and under Article 6 of Convention 108. In turn, medical data are subject to a stricter data-processing regime than non-sensitive data.

Example: In *Z. v. Finland*,[304] 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 that the full judgment and the case documents should remain confidential for 10 years despite requests from the applicant for a longer period of confidentiality. These requests were refused by the court of appeal, 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 granting access to the applicant's identity and medical condition as described in the court of appeal's judgment after a period of only 10 years after passing the judgment would violate Article 8 of the ECHR.

304 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.

Article 8 (3) of the Data Protection Directive 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.[305]

The CoE Medical Data Recommendation of 1997 applies the principles of Convention 108 to data processing in the medical field in more detail.[306] The proposed rules are in line with those of the Data Protection Directive 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.[307]

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 2.1.3.

Intensive discussion has been taking place at the national and European levels on initiatives to store data on the medical treatment of a patient in an electronic health file.[308] A special aspect of having nationwide systems of electronic health files is

305 See also ECtHR, *Biriuk v. Lithuania*, No. 23373/03, 25 November 2008.

306 CoE, Committee of Ministers (1997), Recommendation Rec(97)5 to member states on the protection of medical data, 13 February 1997.

307 ECtHR, No. 1585/09, *Avilkina and Others v. Russia*, No. 1585/09, 6 June 2013, para. 53 (not final).

308 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.

their availability across borders: a topic of particular interest within the EU in the context of cross-border healthcare.[309]

Another area under discussion concerning new provisions is clinical trials, in other words trying out new drugs on patients in a documented research environment; again, this topic has considerable data protection implications. Clinical trials on medical products for human use are regulated by Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use (*Clinical Trials Directive*).[310] In December 2012, the European Commission proposed a regulation to replace the Clinical Trials Directive with the aim of making trial procedures more uniform and efficient.[311]

There are many other legislative and other initiatives pending at the EU level regarding personal data in the health sector.[312]

8.4. Data processing for statistical purposes

Key points

- Data collected for statistical purposes may not be used for any other purpose.
- Data collected legitimately for any purpose may be further used for statistical purposes, provided that national law prescribes adequate safeguards which are met by the users. For this purpose, particularly anonymisation or pseudonymisation before transmission to third parties should be envisaged.

309 Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, OJ 2011 L 88.

310 Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use, OJ 2001 L 121.

311 European Commission (2012), *Proposal for a Regulation of the European Parliament and of the Council on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC*, COM(2012) 369 final, Brussels, 17 July 2012.

312 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.

In the Data Protection Directive, processing data for statistical purposes is mentioned in the context of possible exemptions from data protection principles. In Article 6 (1) (b) of the directive, the principle of purpose limitation may be waived under national law in favour of the further use of data for statistical purposes, although national law must also lay down all necessary safeguards. Article 13 (2) of the directive allows for limitations of access rights by national law if data are processed exclusively for statistical purposes; again, adequate safeguards must exist under national law. In this context, the Data Protection Directive sets up a specific requirement that none of the data acquired or created in the course of statistical research may be used for concrete decisions about data subjects.

Although data which were lawfully collected by a controller for any purpose may be re-used by this controller for their own statistical purposes – so-called secondary statistics – the data would have to be anonymised or pseudonymised, depending on the context, before transmitting them to a third party for statistical purposes, unless the data subject consented to it or it is specifically provided for by a national law. This follows from the requirement of appropriate safeguards under Article 6 (1) (b) of the Data Protection Directive.

The most important cases of using data for statistical purposes are official statistics, performed by the national and EU statistics bureaus based on national and EU laws on official statistics. According to these laws, citizens and businesses are usually obliged to disclose data to the statistics authorities. Officials working in statistics bureaus are bound by special professional secrecy obligations which are carefully observed, as they are essential for the high level of citizen trust which is necessary if data are to be made available to the statistics authorities.

Regulation (EC) No. 223/2009 on European statistics (*European Statistics Regulation*) contains essential rules for data protection in official statistics and may, therefore, also be considered relevant for provisions on official statistics at the national level.[313]

313 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.

The Regulation maintains the principle that official statistical operations need a sufficiently precise legal basis.[314]

> Example: In *Huber v. Germany*,[315] the CJEU found that the collection and storage of personal data by an authority for statistical purposes was not a sufficient reason in itself for processing to be lawful. The law providing for the processing of personal data also needed to meet the requirement of necessity, which was not the case in the given context.

In the context of the CoE, the Statistical Data Recommendation which was issued in 1997 covers the performance of statistics in the public and private sectors.[316] This recommendation introduced principles which coincide with the main rules of the Data Protection Directive described above. More detailed rules are given concerning the following issues.

Whereas data which were collected by a controller for statistical purposes may not be used for any other purpose, data which were collected for non-statistical purpose shall be available for further statistical use. The Statistical Data Recommendation even allows for communicating data to third parties if 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 substitute for the data subject's consent, it is to be assumed that there must be additional 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 transmission.

The people dealing professionally with statistical research should be bound by special professional secrecy obligations – as is typical for official statistics – under national law. This should be extended also to interviewers, if they are employed in collecting data from data subjects or other persons.

If a statistical survey using personal data is not prescribed by law, the data subjects would have to consent to the use of their data in order to make it legitimate, or

314 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; available at: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

315 CJEU, C-524/06, *Huber v. Germany*, 16 December 2008; see especially para. 68.

316 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.

they should at least be given an opportunity to object. If personal data are collected for statistical purposes by interviewing persons, these persons must be clearly informed whether or not disclosing data is mandatory under national law. Sensitive data should never be collected in in such a way that an individual can be identified unless explicitly permitted by national law.

Where a statistical survey cannot be performed without anonymous data, and personal data are indeed necessary, the data collected for this purpose should be anonymised as soon as feasible. The results of the statistical survey must not, at the least, allow for the identification of any data subjects, unless this would manifestly present no risk.

After the statistical analysis has been concluded, the personal data used should either be deleted or rendered anonymous. In this case, the Statistical Data Recommendation proposes that identification data should be stored separately from other personal data. This means, for instance, that the data should be pseudonymised and either the encryption key or the list with the identifying synonyms should be stored separately from the pseudonymised data.

8.5. Financial data

Key points

- Although financial data are not sensitive data in the sense of Convention 108 or of the Data Protection Directive, their processing needs particular safeguards to ensure accuracy and data security.
- Electronic payment systems need built-in data protection, so-called privacy by design.
- Particular data protection problems arise in this area from the need to have appropriate mechanisms for authentication in place.

Example: In *Michaud v. France*,[317] 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

317 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.

report to the administrative authorities information concerning another person which came into their possession through exchanges with that person 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. Since lawyers were subject to the obligation to report suspicions only under very limited circumstances, the ECtHR held that this obligation was proportionate, concluding that there had not been a violation of Article 8.

An application of the general legal framework for data protection, as contained in Convention 108, to the context of payments was developed by the CoE in Recommendation Rec(90)19 of 1990.[318] This recommendation clarifies the scope of lawful collection and use of data in the context of payments, especially by means of payment cards. It further proposes to the domestic legislators detailed regulations on the limits of communicating payment data to third parties, on time limits for the conservation of data, on transparency, data security and transborder data flows and, finally, on supervision and remedies. The solutions proposed correspond to what was later provided as the EU's general data protection framework in the Data Protection Directive.

A number of legal instruments are being created for regulating markets in financial instruments and the activities of credit institutions and investment firms.[319] Other

318 CoE, 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.

319 European Commission (2011), *Proposal for a Directive of the European Parliament and of the Council on markets in financial instruments repealing Directive 2004/39/EC of the European Parliament and of the Council*, COM(2011) 656 final, Brussels, 20 October 2011; European Commission (2011), *Proposal for a Regulation of the European Parliament and of the Council on markets in financial instruments and amending Regulation [EMIR] on OTC derivatives, central counterparties and trade repositories*, COM(2011) 652 final, Brussels, 20 October 2011; European Commission (2011), *Proposal for a Directive of the European Parliament and of the Council on the access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms and amending Directive 2002/87/EC of the European Parliament and of the Council on the supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate*, COM(2011) 453 final, Brussels, 20 July 2011.

legal instruments assist in fighting insider dealing and market manipulation.[320] The most critical issues in these areas which impact on data protection are:

- the retention of records on 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
- the cooperation between competent authorities of Member States and the European Securities and Markets Authority (ESMA).

There are also other issues in these areas that are specifically addressed, including collecting data on the financial status of data subjects[321] or cross-border payment via banking transfers, which inevitably leads to personal data flows.[322]

320 European Commission (2011), *Proposal for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation (market abuse)*, COM(2011) 651 final, Brussels, 20 October 2011; European Commission (2011), *Proposal for a Directive of the European Parliament and of the Council on criminal sanctions for insider dealing and market manipulation*, COM(2011) 654 final, Brussels, 20 October 2011.

321 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; European Commission, *Proposal for a Regulation of the European Parliament and of the Council on amending Regulation (EC) No. 1060/2009 on credit rating agencies*, COM(2010) 289 final, Brussels, 2 June 2010.

322 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.

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.

EDRi, *An introduction to data protection*, Brussels, available at: www.edri.org/files/paper06_datap.pdf.

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, available at: http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R. and Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Chapter 2

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.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

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.

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*, available at: www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

Chapters 3 to 5

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.

Dammann, U. and Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (European Union Agency for Fundamental Rights) (2010), *Data Protection in the European Union: the role of National Data Protection 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.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*, available at: www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

Chapter 6

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.

Chapter 7

Europol (2012), *Data Protection at Europol*, Luxembourg, Publications Office, available at: www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, The Hague, Eurojust.

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.

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, available at: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

Chapter 8

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.

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
Odièvre v. France [GC], No. 42326/98, 13 February 2003

Balancing data protection with freedom of expression

Axel Springer AG v. Germany [GC], No. 39954/08, 7 February 2012
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

Challenges in online data protection

K.U. v. Finland, No. 2872/02, 2 December 2008

Correspondence

Amann v. Switzerland [GC], No. 27798/95, 16 February 2000
Bernh Larsen Holding AS and Others v. Norway, No. 24117/08, 14 March 2013

Cemalettin Canli v. Turkey, No. 22427/04, 18 November 2008
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
McMichael v. the United Kingdom, No. 16424/90, 24 February 1995
M.G. v. the United Kingdom, No. 39393/98, 24 September 2002
Rotaru v. Romania [GC], No. 28341/95, 4 May 2000
S. and Marper v. the United Kingdom, Nos. 30562/04 and 30566/04, 4 December 2008
Shimovolos v. Russia, No. 30194/09, 21 June 2011
Turek v. Slovakia, No. 57986/00, 14 February 2006

Criminal record databases

B.B. v. France, No. 5335/06, 17 December 2009
M.M. v. the United Kingdom, No. 24029/07, 13 November 2012

DNA databases

S. and Marper v. the United Kingdom, Nos. 30562/04 and 30566/04, 4 December 2008.

GPS data

Uzun v. Germany, No. 35623/05, 2 September 2010

Health data

Biriuk v. Lithuania, No. 23373/03, 25 November 2008
I. v. Finland, No. 20511/03, 17 July 2008
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
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

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
Copland v. the United Kingdom, No. 62617/00, 3 April 2007
Cotlet v. Romania, No. 38565/97, 3 June 2003
Kruslin v. France, No. 11801/85, 24 April 1990
Lambert v. France, No. 23618/94, 24 August 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
Halford v. the United Kingdom, No. 20605/92, 25 June 1997
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

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

Right to object

Leander v. Sweden, No. 9248/81, 26 March 1987
Mosley v. the United Kingdom, No. 48009/08, 10 May 2011
M.S. v. Sweden, No. 20837/92, 27 August 1997
Rotaru v. Romania [GC], No. 28341/95, 4 May 2000

Sensitive categories of data

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, Nos. 30562/04 and 30566/04, 4 December 2008

Supervision and enforcement (role of different actors, including data protection 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 "21 Décembre 1989" and Others v. Romania, Nos. 33810/07 and 18817/08, 24 May 2011
Bykov v. Russia [GC], No. 4378/02, 10 March 2009
Kennedy v. the United Kingdom, No. 26839/05, 18 May 2010
Klass and Others v. Germany, No. 5029/71, 6 September 1978
Rotaru v. Romania [GC], No. 28341/95, 4 May 2000
Taylor-Sabori v. the United Kingdom, No. 47114/99, 22 October 2002
Uzun v. Germany, No. 35623/05, 2 September 2010
Vetter v. France, No. 59842/00, 31 May 2005

Video surveillance

Köpke v. Germany, No. 420/07, 5 October 2010
Peck v. the United Kingdom, No. 44647/98, 28 January 2003

Voice samples

P.G. and J.H. v. the United Kingdom, No. 44787/98, 25 September 2001
Wisse v. France, No. 71611/01, 20 December 2005

Selected case law of the Court of Justice of the European Union

Jurisprudence related to the Data Protection Directive

C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, 16 December 2008
[Concept of 'journalistic activities' within the meaning of Article 9 Data Protection Directive]

Joined cases C-92/09 and C-93/09, *Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, 9 November 2010
[Proportionality of the legal obligation to publish personal data about the beneficiaries of certain EU agricultural funds]

C-101/01, *Bodil Lindqvist*, 6 November 2003
[Legitimacy of publishing data by a private person on the private life of others on the internet]

C-131/12, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*, Reference for a preliminary ruling from the *Audiencia Nacional* (Spain) lodged on 9 March 2012, 25 May 2012, pending
[Obligations of search engine providers to refrain, on request of the data subject, from showing personal data in the search results]

C-270/11, *European Commission v. Kingdom of Sweden*, 30 May 2013
[Fine for not implementing a directive]

C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, 29 January 2008
[Obligation of internet access providers to disclose identity of users of KaZaA file exchange programmes to intellectual property protection association]

C-288/12, *European Commission v. Hungary*, 8 April 2014
[Legitimacy of removal of office of the national data protection supervisor]

C-291/12, *Michael Schwarz v. Stadt Bochum*, Opinion of the Advocate General, 13 June 2013
[Violation of EU primary law by Regulation (EC) 2252/2004 providing that fingerprints have to be stored in passports]

Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitling and Others v. Ireland*, 8 April 2014
[Violation of EU primary law by the Data Retention Directive]

C-360/10, *SABAM v. Netlog N.V.*, 16 February 2012
[Obligation of social network providers to prevent unlawful use of musical and audio-visual works by network users]

Joined cases C-465/00, C-138/01 and C-139/01, *Rechnungshof v. Österreichischer Rundfunk and Others and Neukomm and 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]

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-518/07, *European Commission v. Federal Republic of Germany*, 9 March 2010
[Independence of a national supervisory authority]

C-524/06, *Huber v. Bundesrepublik Deutschland*, 16 December 2008
[Legitimacy of holding data on foreigners in a statistical register]

C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, 5 May 2011
[Necessity of renewed consent]

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-614/10, *European Commission v. Republic of Austria*, 16 October 2012
[Independence of a national supervisory authority]

Jurisprudence related to the EU Institutions Data Protection Regulation

C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd.*, 29 June 2010
[Access to documents]

C-41/00 P, *Interporc Im- und Export GmbH v. Commission of the European Communities*, 6 March 2003
[Access to documents]

F-35/08, *Dimitrios Pachtitis v. European Commission*, 15 June 2010
[Use of personal data in the context of employment in EU institutions]

F-46/09, *V v. European Parliament*, 5 July 2011
[Use of personal data in the context of employment in EU institutions]

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

European Union Agency for Fundamental Rights
Council of Europe – European Court of Human Rights

Handbook on European data protection law

2014 — 199 pp. — 14.8 × 21 cm

ISBN 978-92-871-9934-8 (CoE)
ISBN 978-92-9239-461-5 (FRA)
doi:10.2811/69915

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.

More information on the Council of Europe is available on the Internet at hub.coe.int.

Further information on 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.

10.2811/69915
TK-04-14-319-EN-C

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

The rapid development of information and communication technologies underscores the growing need for the robust protection of personal data – a right safeguarded by both European Union (EU) and Council of Europe (CoE) instruments. Technological advances expand the frontiers of, for example, surveillance, communication interception and data storage; all of these pose significant challenges to the right to data protection. This handbook is designed to familiarise legal practitioners who are not specialised in the field of data protection with this area of law. It provides an overview of the EU's and the CoE's applicable legal frameworks. It explains key jurisprudence, summarising major rulings of both the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU). Where no such case law exists, it presents practical illustrations with hypothetical scenarios. In a nutshell, this handbook aims to help ensure that the right to data protection is upheld with vigour and determination.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS
Schwarzenbergplatz 11 - 1040 Vienna - Austria
Tel. +43 (1) 580 30-60 - Fax +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

COUNCIL OF EUROPE
EUROPEAN COURT OF HUMAN RIGHTS
67075 Strasbourg Cedex - France
Tel. +33 (0) 3 88 41 20 00 - Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

Publications Office
ISBN 978-92-871-9934-8 (CoE)
ISBN 978-92-9239-461-5 (FRA)