Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

T4DATA

The DPO Handbook

Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation

By Douwe Korff and Marie Georges
drawing on major contributions by the project partners
under the **Training Data Protection Authorities and Data Protection Officers - T4DATA** project.
(Grant Agreement number: 769100 — T4DATA — REC-DATA-2016/REC-DATA-2016-01)

Project Partners

Fondazione Lelio e Lisli Basso – ONLUS (Italy)
Coordinator

FONDAZIONE LELIO E LISLI BASSO

and

Garante per la Protezione dei Dati Personali (Italy)

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Agencia de Proteccion de Datos (Spain)

aepd agencia española protección datos

Agencija za zastitu osobnih podataka (Croatia)

azop Agencija za zaštitu osobnih podataka

Commission for Personal Data Protection (Bulgaria)

Комисия за защита на личните данни

Urząd Ochrony Danych Osobowych (Poland)

Urząd Ochrony Danych Osobowych

The DPO Handbook

Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation

(Regulation (EU) 2016/679)

Elaborated for the EU-funded "T4DATA" programme

(Grant Agreement number: 769100 — T4DATA — REC-DATA-2016/REC-DATA-2016-01)

by

Douwe Korff

Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

&

Marie Georges

Independent international data protection expert
(ex-CNIL, EU, Council of Europe, etc.)

Members of the Fundamental Rights Experts Europe (FREE) Group

Drawing on major contributions by the Italian Data Protection Authority & the project partners

(As approved by the Commission,July 2019)

Douwe Korff& Marie Georges

The DPO Handbook

About this Handbook:

This Handbook has been prepared as part of the training materials for the EU-funded "T4DATA" training-of-trainers programme, aimed at training staff in a number of EU Member States' data protection authorities (DPAs) in training of data protection officers (DPOs), especially in the public sector, in their new duties under the EU General Data Protection Regulation (Regulation 2016/679, GDPR). The project is carried out under the wing of the Italian data protection authority, the *Garante per la protezionedeidatipersonali* (hereafter '*Garante'* or '*Garante della Privacy*'), and administered by the *Fondazione Basso*, with the help of two experts from the *Fundamental Rights Experts Europe* (FREE) Group, Mrs. Marie Georges and Prof. Douwe Korff.

The Handbook draws on major contributions from the *Garante della Privacy* and from the other DPA-partners who sent in very useful practical examples and copies of their own guidance notes on the GDPR.

Note that where a matter relates to one of the two experts' previous work, her/his name is in a related footnote only when referring to publicly available resources. This is rarely the case for Marie Georges mainly for institutional or confidential reasons related to her work on data protection for national and international governmental bodies.

For information on the programme, the partners and the experts, see:

http://www.fondazionebasso.it/2015/wp-content/uploads/2018/04/T4Data_Brochure.pdf

Although produced for the T4DATA programme, it is hoped that the Handbook will be useful also to anyone else interested in the application of the Regulation, and in particular other DPOs (in the public- or private sector). it is made publicly available under a "Creative Commons" (CC) license.

Note: Since the handbook aims to support the training of data protection officers (DPOs) in their new duties under the GDPR, it focuseson EU data protection law, and more specifically on data protection law in relation to what used to be called "First Pillar" or "internal market" matters. However, sections 1.3.4 – 1.3.6 and 1.4.3 – 1.4.5 still briefly introduce the data protection rules and instruments that applied or apply to other matters covered by EU law, i.e., matters falling with the area of what used to be called "Justice and Home Affairs" (JHA) or the "Third Pillar" – now referred to as the area of "Freedom, Security and Justice" (FSJ); matters relating to the so-called Common Foreign and Security Policy (CFSP) – the previous "Second Pillar"; and the activities of the EU institutions themselves; and section 1.4.6 discusses data transfers between different EU regimes. Also not covered is data protection outside the EU/EEA, even though we feel that DPOs should acquire at least some knowledge of the major influence that the EU rules have had, and continue to have, on data protection worldwide.

We hope to be able to add those issues in a later, second edition of this handbook, in which we should then also be able to update the information on matters still pending at the time of writing this first edition such as, in particular, developments in relation to the e-Privacy Regulation, which at the time of writing is still going through the legislative process.

The handbook is also available in Italian, Croatian, Bulgarian, Polish, Spanish (i.e., all the partners' languages). Further translations (in particular, a French) translation are under consideration (depending on financing).

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

DISCLAIMER:

The information and views set out in this handbook are those of the authors and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

Reproduction is authorised provided the authors and source are acknowledged.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Foreword

This first edition of the 'Handbook' produced as part of the EU-funded 'T4Data – Training for Data' project is, we believe, something more than 'yet another' manual on the GDPR.

It is truly a hands-on manual that was made possible firstly, thanks to the hard work and commitment shown by the two experts selected for this exercise, M.me Marie Georgesand Professor Douwe Korff, who have long-standing familiarity with human rights, ICT and data protection issues, both conceptual and practical – and secondly, thanks to the knowledgeable contribution of officers and members from the five participating supervisory authorities, who have relied on their daily practice and experience in order to provide meaningful input to the guidance contained in the Handbook.

It is, above all, work in progress, living law, not just dead letter. It is intended to translate the new, unquestionably more demanding tasks of **accountability** set out in the new EU legal framework – which are aimed at ensuring DP efficiency in a world were data processing is exploding in all dimensions of life– into practical, sound, documented guidance and advice that will be adjusted and expanded further thanks to the national training and dissemination activities that will continue throughout 2019 on the foundations of this Handbook. The addressees of this guidance are DPOs, and especially DPOs working in the public sector, who will be able to use it as a sort of stepping stone to strengthen and enhance their competence in handling data protection issues to the benefit of all the stakeholders – controllers, data subjects, and the public at large.

This is why our five authorities decided to join forces with a view to implementing the T4Data Project, and also why we are especially pleased to present this valuable project deliverable, in English and translated into our respective national languages – plus hopefully into French in the near future – knowing it will add a strong link to the chain of cooperation tools we are forging day by day at European level and worldwide.

Edyta Bielak – Jomaa, PhD President of the Personal Data Protection Office in Poland

Mar España Martí, Director of the Spanish Agency of Data Protection

Ventsislav Karadjov, Chairman of the Commission for Personal Data Protection of the Republic of Bulgaria

Anto Rajkovača, Director of the Croatian Personal Data Protection Agency

Antonello Soro – President, Italian Supervisory Authority

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

CONTENTS

Page:

Introduction

PART ONE – The origins and meaning of data protection

1.1 Confidentiality, privacy/private life and data protection: different but but complementary concepts in the age of digitalisation

1.1.1 Confidentiality and privacy/private life
1.1.2 "Data protection"

1.2 The first data protection laws, principles and international instruments

1.2.1 The first data protection laws
1.2.2 The basic principles
1.2.3 The 1981 Council of Europe Data Protection Convention and its Additional Protocol

1.3 European data protection law in the 1990s and early-2000s

1.3.1 Data protection in the European Community
1.3.2 The main 1995 EC Data protection Directive
1.3.3 The 1997 Telecommunications Data Protection Directive, the 2002 EC e-Privacy Directive and the 2009 amendments to the e-Privacy Directive 2002 EC e-Privacy Directive
1.3.4 Third-Pillar data protection instruments
1.3.5 Data protection instruments in the Second Pillar
1.3.6 Data protection rules for the EU institutions

1.4 Data protection law for the future

1.4.1 The EU General Data Protection Regulation of 2016
1.4.2 The proposed EU e-Privacy Regulation
1.4.3 The Law Enforcement Data Protection Directive of 2016
1.4.4 Data protection in relation to the Common Foreign and Security Policy
1.4.5 New data protection rules for the EU institutions
1.4.6 Transfers of personal data between the different regimes
1.4.7 The "Modernised" Council of Europe Data Protection Convention of 2018

PART TWO – The General Data Protection Regulation

2.1 Introduction

2.2 Status and approach of the GDPR: direct applicability with "specification" clauses

2.3 The accountability principle

2.3.1 The new duty to be able to demonstrate compliance
2.3.2 Means of demonstrating compliance
2.3.3 Evidentiary value of the various means of demonstrating compliance

2.4 The Data Protection Officer

2.4.1 Background
2.4.2 The duty to appoint a Data Protection Officer
2.4.3 Qualifications, qualities and position of the DPO
2.4.4 Functions and tasks of the DPO (Overview)

Contents continued overleaf

Contents continued:

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

PART THREE – Practical guidance on the tasks of the DPO or that will in practice involve the DPO ("The DPO Tasks")

Preliminary task:

Scoping the controller's environment

Organisational functions:

Task 1: Creating a register of personal data processing operations

Attachment: Sample format of a detailed personal data processing record

Task 2: Reviewing the personal data processing operations

Task 3: Assessing the risks posed by the personal data processing operations

Task 4: Dealing with operations that are likely to result in a "high risk": carrying out a Data Protection Impact Assessment (DPIA)

Monitoring of compliance functions:

Task 5: Repeating Tasks 1 – 3 (and 4) on an ongoing basis

Task 6: Dealing with personal data breaches

Attachment: Examples of personal data breaches and who to notify

Task 7: Investigation task (including handling of internal complaints)

Advisory functions:

Task 8: Advisory task – general

Task 9: Supporting and promoting "Data Protection by Design & Default"

Task 10: Advise on and monitoring of compliance with data protection policies, joint controller-, controller-controller- and controller-processor contracts, Binding Corporate Rules and data transfer clauses

Task 11: Involvement in codes of conduct and certifications

Cooperation with and consultation of the DPA:

Task 12: Cooperation with the DPA

Handling data subject requests:

Task 13: Handling data subject requests

Information and raising awareness:

Task 14: Information and awareness-raising tasks

Task 15: Planning and reviewing the DPO's activities

- o – O – o -

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation

(Regulation (EU) 2016/679)

Introduction

On 25 May 2018, the new EU General Data Protection Regulation (**GDPR** or "**the Regulation**")[1] came into application, replacing the 1995 Data Protection Directive ("the 1995 Directive").[2] Adopted in response to the massive expansion in the processing of personal data since the introduction of the 1995 Directive, and to the development of ever-more-intrusive technologies, the Regulation builds on the Directive, and on the EU's Court of Justice (CJEU)'s case-law under it. In doing this, it significantly expands on the Directive and, in doing so, considerably strengthens the main EU data protection regime. It brings many changes in terms of much greater harmonisation, stronger data subject rights, closer cross-border enforcement cooperation between data protection authorities (DPAs), etc.

Among the most important changes are the introduction of a new principle, the "accountability" principle, and of the institution of data protection officers (**DPOs**). The two are linked: the DPOs will be the people who in practice will have to ensure compliance with the accountability principle by and within the organisations to which they belong. This Handbook seeks to support the new DPOs in the public sector in that effort.

The Handbook consists of three parts:

- **Part One** introduces the concepts of "confidentiality", "privacy" and "data protection" and the first data protection laws, -principles and international instruments (in particular the 1981 Council of Europe Data Protection Convention), before discussing the EU "First Pillar" data protection directives of the 1990s and early-2000s, and introducing the recently adopted and pending data protection instruments for the future (the GDPR, the proposed e-Privacy Regulation, and the "Modernised" Council of Europe Convention).[3] Part One does not yet discuss the EU's 1990s "Third Pillar" instruments and the data protection rules for the EU's own institutions, and their successors.*

  * It is hoped that in future an expanded, second edition of this Handbook can be produced that will also properly cover those instruments.

---

[1] Full title: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. L 119 of 4.5.2016, p. 1ff., available at:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
Note that although the Regulation was adopted in 2016, and legally came "into force" on the twentieth day following that of its publication in the Official Journal of the European Union, i.e., on 25 May of that year (Article 99(1)), it only came into "application" – i.e., was only effectively applied – from 25 May 2018 (Article 99(2)).

[2] Full title: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23.11.1995, p. 31ff, available at:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en

[3] On the limitations to the matters discussed, see the Note in the box "*About this handbook*" on p. 1.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

- **Part Two** provides an overview of all the key elements of the General Data Protection Regulation, before focussing on the additional, new core "accountability" principle and the concept and rules in the GDPR relating to the Data Protection Officer.
- **Part Three** provides practical guidance on how DPOs in the public sector can and should fulfil their numerous tasks, with real-life examples, relating in particular to the three focus areas: education, finance and health care, and exercises.

Apart from extensive references and links to materials in footnotes, a separate second volume (Volume Two) to the handbook contains extensive further materials that are made available to participants in the "T4DATA" trainings.

Website:

As many as possible of the above-mentioned materials and links will also be made available on the publicly-accessible website that accompanies this Handbook (which is also made freely available under a "Creative Commons" license from the website):

http://www.fondazionebasso.it/2015/t4data-training-data-protection-authorities-and-data-protection-officers/

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

PART ONE

The origins and meaning of data protection

This part seeks to explain what data protection is and how it developed in Europe, and how the new and "modernised" European data protection instruments seek to address the latest technological developments.

- Section 1.1presents the differing (if overlapping) concepts of confidentiality, privacy and private life and data protection and the approach to the latter as developed in Europe, including the human rights- and rule-of-law requirements that, in Europe, underpin data protection.

- Section 1.2 covers the origins of data protection in Europe, the emergence of the basic data protection principles and -rights, and their development in European and global non-binding legal instruments – and into one binding one, the 1981 Council of Europe Data Protection Convention (including its Additional Protocol of 2001).

- Section 1.3 deals with the way in which the data protection rules and principles were further developed in the 1990s and early-2000s (to enable the development of the EU's "Internal Market", which required both the free flow of data and protection of the fundamental right to data protection), with a focus on the 1995 Data Protection Directive (with which the 2001 Additional Protocol to the 1981 Convention sought to align that Convention) (sub-sections 1.3.1 and 1.3.2); and discusses the special rules for the telecommunication sector (sub-section 1.3.3).

  The final sub-sections in this section briefly note the data protection instruments in what used to be called the Justice and Home Affairs (JHA) area (sub-section 1.3.4); in relation to the Common Foreign and Security Policy (CFSP) (sub-section 1.3.5); and for the EU institutions themselves (sub-section 1.3.6).

- Section 1.4 introduces the latest legal instruments, adopted to meet the future: the 2016 EU General Data Protection Regulation (GDPR, in application since 25 May 2018) (sub-section 1.4.1) and the proposed replacement of the 2002 EC e-Privacy Directive with an e-Privacy Regulation (sub-section 1.4.2).

  The next sub-sections in this section briefly note the main new data protection instrument in what is now called the area of Justice, Freedom and Security (JFS), the 2016 Law Enforcement Data Protection Directive (LEDPD) (sub-section 1.4.3); the situation in relation to the CFSP (sub-section 1.4.4); and the update to the data protection instrument for the EU institutions, Regulation 2018/1725 (sub-section 1.4.5). Sub-section 1.4.6 discusses data flows between the different EU data protection regimes.

  The "Modernised" Council of Europe Convention, opened for signature in October 2018, is discussed in the final sub-section (sub-section 1.4.7).

  NB: We hope topresent the EU data protection instruments for the areas mentioned above (law enforcement and judicial cooperation, CSFP, and the EU's own institutions), adopted to replace those of the 1990s and early-2000s, and the latest global rules, in more detail in a second edition.

The GDPR, being at the heart of this handbook, is further examined in Part Two.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

1.1 Confidentiality, privacy/private life and data protection: different but complementary concepts in the age of digitalisation

1.1.1 Confidentiality and privacy/private life

There have always been areas in which personal information was treated as subject to special rules of **confidentiality**. The classical examples are the Hypocratic Oath for **medical doctors,**[4]and the Roman Catholic Church's "**seal of the confessional**".[5] More recently,in particular from the 19th Century, **bankers, lawyers**, other **ministers of religion**, **postal- and telecommunication workers** and many others have been required to treat the information they receive from individuals in their official capacity as confidential, privileged,[6] or even sacrosanct.

Such duties of confidentiality were generally seen as serving both the individual and society: the individual could have faith in the person to whom he or she disclosed the information treating the information confidentiality, and such trust in turn served the public good, in that its absence can deter people from seeking help or revealing information to the authorities, which undermines public health and other social benefits, e.g., in trying to counter the spread of sexually transmitted diseases or political or religious extremism.

However, as Frits Hondius, deputy director of human rights at the Council of Europe and in charge of the drafting of the first internationally-binding data protection instrument, the 1981 Council of Europe Data Protection Convention, discussed at 1.2.3, below) explains, although there was this duty of confidentiality resting on them:[7]

> there was no corresponding right vested in patients, clients or citizens to check the accuracy and relevance of data concerning them. And while legal sanctions existed to punish gross abuses of data handling, there were no laws providing positive indications as to how personal data files should be properly set up and managed.

---

[4] The Hippocratic Oath was attributed to Hippocrates (c. 460-370 BC) in antiquity although new information shows it may have been written after his death. A The oldest existing version dates from circa 275 AD and is as follows: ἃ δ' ἀνένθεραπείῃ ἴδω ἢ ἀκούσω, ἢ καὶ ἄνευθεραπείης κατὰ βίονἀνθρώπων, ἃ μὴχρή ποτεέκλαλεῖσθαι ἔξω, σιγήσομαι, ἄρρητα ἡγεύμενοςεἶναι τὰτοιαῦτα. "*And whatsoever I shall see or hear in the course of my profession, as well as outside my profession in my intercourse with men, if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets*." (Translation by James Loeb, 1923). See:
https://en.wikipedia.org/wiki/Hippocratic_Oath

[5] In the Roman Catholic Church, the "seal of the confessional" or "sacramental seal" is inviolable. See:
https://www.catholiceducation.org/en/religion-and-philosophy/catholic-faith/the-seal-of-the-confessional.html

[6] As the Solicitors Regulation Authority (SRA), regulating solicitors and law firms in England and Wales, puts it, there is (in English law) a "difference between confidentiality and legal professional privilege. In brief terms, confidential information may be disclosed where it is appropriate to do so but privilege is absolute, and privileged information cannot therefore be disclosed. Confidential communications between lawyers and clients for the purpose of obtaining and giving legal advice are privileged."
https://www.sra.org.uk/solicitors/code-of-conduct/guidance/guidance/Disclosure-of-client-confidential-information.page
In France, a lawyer's (*avocat*) professional secrecy (*secret professionnel*) is a matter of *ordre public*, absolute, unlimited in time and covering all types of legal matters and any form of information (written, electronic, audio, etc.). See:
http://www.avocatparis.org/mon-metier-davocat/deontologie/secret-professionnel-et-confidentialite

[7] Frits Hondius, *A decade of international data protection*, in:Netherlands International Law Review, Vol. XXX (1983), pp. 103 – 128 (not available online).

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

A right to "**privacy**" or "**respect for private life**" was enshrined in the post-WWII international human rights treaties, the UN International Covenant on Civil and Political Rights (ICCPR, Art. 17) and the European Convention on Human Rights (ECHR, Art. 8).[8] It protects primarily against unnecessary interferences by the state in a person's private life, such as interception of communications by state agencies[9] or the criminalisation of private sexual acts.[10]However, the right has also been interpreted by the European Court of Human Rights as requiring the state to protect individuals against the publication of photographs taken of them by private entities, without their consent, in a private setting,[11] and against interception of their communications by their employers without proper legal basis.[12]

Still, while Article 8 ECHR has more recently increasingly been interpreted and applied so as to also protect individuals in respect of their personal data, and in relation to the collection, use and retention of such data on them, especially by state and national security agencies,[13] in the 1970s and 80s, the extent to which the right to private life could be relied upon in relations between individuals, and between individuals and private entities (the so-called question of "horizontal effect of human rights" or *Drittwirkung*) was still very unclear[14] – and has still not been fully resolved in terms of traditional human rights law. In any case, individuals cannot derive from the ECHR (or the ICCPR) a right of action against other individuals – the most they can do is to take action against the relevant state-party for failing to protect them, in relevant domestic law, against the actions of such other individuals.

In sum: The laws and rules on confidentiality, professional privilege and secrecy, and the human rights guarantees of privacy and private life did not, and do not, adequately protect individuals against abusive collection and use of their personal data.

Consequently, more recently, a separate and distinct right to "**protection of personal data**" ("data protection") has become recognised, as is discussed next. But of course, this new *sui generis* right must always be seen as closely linked to and complementary to the traditional rights – as enshrined in the ECHR and ICCPR in particular: data protection seeks to ensure the full and effective application of the traditional rights in the (relatively) new digital

---

8 Article 12 of the 1948 Universal Declaration of Human Rights, which was the "mother" instrument to both the ICCPR and the ECHR (but which itself is not a binding treaty), already stipulated in Article 12 that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence …" The ICCPR and ECHR were drafted in parallel in 1949-50 (but the ECHR, which was opened for signature at the end of 1950 and entered into force in 1953, came into force more than twenty years before the ICCPR, which was opened for signature in 1966 and entered into force only in 1976).

9 E.g., ECtHR, *Klass v. Germany*, judgment of [ADD DATE].

10 E.g., ECtHR, *Dudgeon v. the UK*, judgment of [ADD DATE].

11 E.g., ECtHR, *von Hannover v. Germany*, judgment of [ADD DATE].

12 E.g., ECtHR, *Halford v. the UK*, judgment of 25 June 1997.

13 See the Council of Europe Factsheet – Personal Data Protection, 2018, available at: https://www.echr.coe.int/Documents/FS_Data_ENG.pdf
A non-exhaustive list of cases of the European Court of Human Rights relating to personal data protection is available at:
https://www.coe.int/en/web/data-protection/echr-case-law
For a more general discussion, see Lee A Bygrave, *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*, International Journal of Law and Information Technology, 1998, volume 6, pp. 247–284, available at:
https://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/Human_rights.pdf

14 See Hondius, o.c. (footnote 7, above), p. 107, with reference to the Report by the Committee of Experts on Human Rights, Council of Europe (DH/EXP(70)15).

context.

1.1.2 "Data protection"

Computers were first built for military purposes in **War World II**. The UK code-breakers, under the leadership of the great Alan Turing,[15] built primitive versions for the decrypting of German *Enigma*- and *Lorenz*-encoded messages.[16] In the USA, IBM, under the leadership of its first CEO, Thomas J Watson, produced large quantities of data processing equipment for the military and began to experiment with analog computers.[17] And the Germans used them for calculating the trajectory of *V2* rocket missiles[18].

The need to protect human rights and freedoms in a democracy in relation to automated personal data processing emerged only later when, in the **1960s**, computers started to be used for management purposes in the public and private sectors. But because of the high cost of computers and the large space they required at that time, this was only done in developed countries, and even there only for large public authorities and -companies. The first uses of computers related to the payment of salaries and providers, patients register in hospitals, public census and statistics – and police files.

In the light of these developments, at **the end of 1960s/beginnings of the 1970s**, the same debates started to take place in Germany (in particular, in the *Land* of Hessen, about police files), Norway, Sweden and France (in particular because of memories of the abuse of population- and other public registers by the Nazi occupiers in WWII), the UK, the USA, etc. – and at the OECD and the Council of Europe.[19] At first those debates were held between professionals under ethical obligations (in the USA, in particular among medical doctors and IT engineers, who were the first to produce guidelines on "Fair Information Practices")[20] and among politicians who were concerned about the risks of abuse or misuse or security of personal data processed automatically.

---

[15] See:
http://www.maths.manchester.ac.uk/about-us/history/alan-turing/

[16] See: Chris Smith, *Cracking the Enigma code: How Turing's Bombe turned the tide of WWII*, 2 November 2017, available at:
http://home.bt.com/tech-gadgets/cracking-the-enigma-code-how-turings-bombe-turned-the-tide-of-wwii-11363990654704
The *Colossus* machine used to decode the *Lorenz* messages is generally regarded as "the world's first programmable, electronic, digital computer". See:
https://en.wikipedia.org/wiki/Colossus_computer

[17] See:
https://en.wikipedia.org/wiki/Thomas_J._Watson

[18] See: Helmut Hoelzer's Fully Electronic Analog Computer used in the German V2 (A4) rockets (mainly in German), available at:
http://www.cdvandt.org/Hoelzer%20V4.pdf

[19] The Council of Europe adopted its first resolutions on the issues in 1973 and 1974: Committee of Ministers' Resolutions (73)22 and (74)29 (for links, see footnotes 39 and 40, below). See the Explanatory Memorandum to the 1981 Council of Europe Data Protection Convention, para. 6, available at:
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434
The principles adduced in those resolutions are included in Attachment 1 to the handbook.

[20] See: Robert Gellman, Fair Information Practices: A basic history, available at:
https://bobgellman.com/rg-docs/rg-FIPshistory.pdf
For many years, from the 1970s to the 1990s, Gellman worked on U.S. legislative privacy matters in the House of Representatives.

They then, in the **mid- andlate-1970s and early-80s**, spread to the wider populations – in France, an early major catalyst was the 1974 exposure by whistleblowers of government plans to set up a national database of all French nationals and residents with a unique identification number for each of them; and of the existence of contentious police files [21] In Germany, there was widespread opposition, in a generally tense political climate, to the proposed national census of 1983.[22] Those debates were not just about the risk of infringement of privacy made possible by the use of new technologies, but also about the consequences of data mistakes, and about possible authoritarian power created by centralising data collected for different purposes and/or using unique identifiers for interconnecting files. In Europe, they led to a demand for specific, statutorily-underpinned "data protection" or "informatics and liberties", reinforced by increasing recognition of this need by constitutional and other highest courts, and to the adoption of international instruments (as discussed in section 1.2, below).

The term "data protection" (German: ***Datenschutz***) was originally coined in the title of the very first law on the subject, the 1970 Data Protection Law (*Datenschutzgesetz*) of the German State of Hessen, drafted by "the father of data protection", Prof. Spiros Simitis.[23] As Burkert points out, the title was actually "a misnomer, since [the Law] did not protect data but the rights of persons whose data [were] being handled."[24]

But it stuck: the term – now famous the world over and shining as a star over the world (the French now also refer to ***protection des données***) – is shorthand for "the protection of individuals with regard to the processing of personal data" (the longhand phrase used in the titles of both the 1995 EC Data Protection Directive and the 2016 EU General Data Protection Regulation).[25] But even this fuller phrase does not quite clarify the meaning of the concept in European eyes and minds.

Data protection has both individual freedom- and societal aspects.

Thus, in France (where the law uses the phrase "*informatics, files and liberties*"/"*informatique, fichiers et libertés*"), data protection is seen as part of the dual individual- and societal and constitutional requirements that:

---

[21] See the article in the newspaper Le Monde of 21 of March 1974, "*SAFARI ou la chasse aux Français*" ("SAFARI, or the hunt for the French"), available at:
http://rewriting.net/2008/02/11/safari-ou-la-chasse-aux-francais/
The name of the database, SAFARI, was an acronym for "*systèmeautomatisé pour les fichiersadministratifs et le répertoire des individus*" (Automated system for administrative dossiers and file collections on individuals), but was also chosen because of the Minister In charge of that project loved to go on safari in Africa. The revelation was covered by all other newspapers the following days, and the government stopped the project some days later, appointing an *ad hoc* commission to study the whole problem and suggest legal solutions.

[22] See: Marcel Berlinghoff, *Zensus und Boykott. Die Volkszählungvor 30 Jahren*, in: Zeitgeschichte-online, June 2013, available at:
https://zeitgeschichte-online.de/kommentar/zensus-und-boykott-die-volkszaehlung-vor-30-jahren

[23] *HessischesDatenschutzgesetz (HDSG) 1970*, in force from 13 October 1970, *Gesetz- und Verordnungsblatt für das Land Hessen, Teil I*, 1970, Nr. 41 (12 October 1970), p. 625ff, original text (in German) available at:
http://starweb.hessen.de/cache/GVBL/1970/00041.pdf

[24] Herbert Burkert, Privacy-Data Protection: A German/European Perspective (undated, approximately 2000), p. 46, available at:
http://www.coll.mpg.de/sites/www/files/text/burkert.pdf

[25] The GDPR uses "natural persons" instead of "individuals".

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

> **Informatics must be at the service of each citizen. … It may not endanger human identity, human rights, private life, or individual or public liberties**[26]
>
> (Art. 1 of the 1978 *Law on Informatics, Files and Freedoms*)

That French law gained constitutional status, and the country's highest courts' decisions are based on privacy or freedom, depending on the issues at stake.

In Germany, data protection is primarily seen as derived from the fundamental (proto-)right to "[respect for] the human personality" (*das allgemeinePersönlichkeitsrecht*), guaranteed by Art. 2(1) of the Constitution, read together with Art. 1(1). From this, the Constitutional Court, in its famous *Census* judgment of 1983, derived a more specific right to "**informational self-determination**" (*informationelleSelbstbestimmung*).[27] However, the *Bundesverfassungsgericht* still clearly and strongly linked this individual right to wider, fundamental societal norms:[28]

> A social and legal order in which the citizen can no longer know who knows what, and when, about him and in which situation, is incompatible with the right to informational self-determination. A person who wonders whether unusual behaviour is noted each time and thereafter always kept on record, used or disseminated, will try not to come to attention in this way. A person who assumes, for instance, that participation in a meeting or citizen initiative is officially recorded, and may create risks for him, may well decide not to exercise the relevant fundamental rights ([as guaranteed in] Articles 8 and 9 of the Constitution). This would not only limit the possibilities for personal development of the individual, but also the common good, because self-determination is an essential prerequisite for a free and democratic society that is based on the capacity and solidarity of its citizens.

Other European states, while readily accepting the need for data protection, and indeed often enshrining it in their constitutions as a *sui generis* right,[29] have not all adopted the German concept of informational self-determination – often precisely because they feel it puts too much emphasis on the individual freedom aspect and not enough on the wider societal ones.[30]Still, basically, in Europe all agree that, as Hondius already put it in 1983:[31]

---

[26] "*L'informatique doit être au service de chaque citoyen. ... Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.*" The omitted sentence stipulates that "[Data protection] is to be developed within the framework of international cooperation".

[27] BVerfG, 15.12.1983, BVerfGE Bd. 65, S. 1 ff. On the issue of "informational self-determination", see § 151ff.

[28] *Idem*, § 154 (our translation).

[29] Cf. the 1978 Austrian data protection law, which contains a "constitutional" provision in its first article, declaring data protection to be a constitutionally-protected right. Data protection is also expressly provided for in the constitutions of countries that became democratic in this era, such as Spain (Art. 18-4), Portugal (Art. 35), Greece (Art. 9A), Hungary (Art. 59), Lithuania (Art. 22), Slovenia (Art. 38), Slovakia (Art. 19), or that revised their constitution to reflect modern society, such as the Netherland (Art. 10).

[30] See, e.g., the blog *InformationelleSelbstbestimmung - (noch) keinneuesGrundrecht*, 26 October 2017, on the refusal of the lower house of the Swiss Federal Parliament (*Nationalrat*) to enshrine the principle of informational self-determination in the Swiss Federal Constitution: https://www.humanrights.ch/de/menschenrechte-schweiz/inneres/person/datenschutz/informationelle-selbstbestimmung

In the Netherlands, too, the principle has not been adopted in law or by the courts – even though apart from that, the highest court, the *Hoge Raad*, has been influenced by the case-law of the German Constitutional Court. See: T. F. M. Hooghiemstra, Tekstentoelichting Wet beschermingpersoonsgegevens (2001), section 4.3 (p. 18).

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

> Data protection aims at safeguarding a just and reasonable equilibrium between the interests of the individuals and those of the community [in relation to the processing of personal data].

The European states took the view that, in order to achieve this equilibrium, the following **regulatory principles** should apply:

- the collection and further use and disclosure of personal data should be subject to **law** (i.e., to **binding legal rules**, rather than voluntary codes or non-binding guidelines);[32]
- those laws should be **"omnibus" laws** that in principle apply to all public and private entities that process personal data (with exceptions and modifications of those rules and principles provided for in special rules as and when this is necessary, but always respecting their "essential core");
- the law in question must contain certain **core substantive rules** (reflecting the **"core" data protection principles** discussed under the next heading) and grant data subjects **crucialindividual rights**; and
- the application of those laws should be overseen by **special supervisory bodies** (usually referred to as **data protection authorities** or **DPAs**).

1.2 The first data protection laws, principles and international instruments[33]

1.2.1 The first data protection laws

> **"Western Europe is the cradle of data protection"**[34]

As mentioned, the very first data protection law in the world was the***Datenschutzgesetz* of the German State of Hessen, adopted in September 1970**.[35] That law also introduced the first independent data protection authority (albeit, because of state competence issues, only for the public sector and with limited powers of mediation rather than enforcement).

The Hessen Data Protection Law was followed, in Europe, in that decade, by the adoption of national (nationwide) data protection laws in **Sweden (1973)**, the first **German Federal Data**

---

31 Hondius, o.c. (footnote 7, above), p. 108.

32 Cf. the interpretation of the concept of "law" in the European Convention on Human Rights (in particular Article 8 – 11), by the European Court of Human Rights.

33 For historical details, with particular reference to the drafting in parallel of the 1980 OECD Guidelines and the 1981 Council of Europe Data Protection Convention, and to the then already appearing differences of views between Europe and the USA, see: Frits Hondius, o.c. (footnote 7, above), pp. 103 – 128, and the Explanatory Memorandum to the Council of Europe Convention, o.c. (footnote 19, above), para. 14. A very useful general overview of the historical developments on privacy is provided in Chapter 4 of the updated OECD Privacy Framework, headed *The evolving privacy landscape: 30 years after the OECD Privacy Guidelines*, further discussed below (see footnote 41, below). A fascinating personal account of the background to the drafting of the OECD Guidelines and the politics (Europe vs. USA) and personalities involved (including Frits Hondius, Louis Joinet, Stefano Rodotà and Spiros Simitis), is provided in Michael Kirby, Privacy Today: Something Old, Something New, Something Borrowed, Something Blue, Journal of Law, Information and Science, 2017 25(1), available at: http://www.austlii.edu.au/au/journals/JlLawInfoSci/2017/1.html

34 Hondius, o.c. (footnote 7, above), p. 104, with reference to the early laws noted in the text.

35 See footnote 23, above. For further references on the history of data protection in Germany, see: Herbert Burkert, o.c. (footnote 24, above).

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Protection Law (end of 1977) (which covered personal data processing by federal agencies and by the private sector), the **French *Informatics, files and Freedoms Law* of 6 January 1978**, laws in **Austria**, **Denmark**[36] and **Norway(all also 1978)** and **Luxembourg (1979)**. Although some of these, such as the German Federal Law, contained separate sets of rules for the federal public- and private sectors, they are still "omnibus" laws, because the rules for both sectors are based on the same basic principles and rights, often derived from the constitution.[37]

1.2.2 The basic principles

The 1970 laws in Europe coalesced around an increasingly generally-accepted (broadly-phrased) **set of"core" principles and rights**. They were similar to the basic *Fair Information Practices* principles drafted at around the same time in the USA (although these were less detailed and not set out in binding law).[38]

These core principles of the early laws in Europe were in turn reflected in **the earliest (non-binding) European instruments** on the issue, issued by the Council of Europe (and which in turn became the basis for the later, binding Council of Europe Data Protection Convention):

- 1973 Council of Europe Resolution (73)22 on The Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector, adopted by the Committee of Ministers on 26 September 1973;[39]
- 1974 Council of Europe Resolution (74)29 on The Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector, adopted by the Committee of Ministers on 20 September 1974.[40]

The "core" principles were next recognised in **global international, but still non-binding instruments**, i.e.:

- the 1980 OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data;[41] and

---

[36] In Denmark, there were initially two laws, one for the private sector and one for the public sector, adopted on the same day (Laws Nos. 293 and 294, both of 8 June 1978), but still both based on the same broad principles. For background, see the *Introduction* in: Peter Blume, Personregistrering, Copenhagen, 1991. They remained in force, with various amendments, until 2000, when new legislation was put into place to implement the 1995 EC Data Protection Directive.

[37] The separate state data protection laws (*Landesdatenschutzgesetze*) cover the state public sectors, but are based on the same principles, rooted in the Constitution.

[38] See sub-section 1.3.4, below.

[39] Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502830

[40] Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c51

[41] OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980, available at: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
For background, see Kirby, o.c. (footnote 33, above).

- the 1989 UN Guidelines for the Regulation of Computerized Personal Data Files, adopted by the UN General Assembly (UNGA).[42]

For the full text of the basic principles in the above four non-binding international instruments from the 1970s and 80s, and the 1973 U.S. *Fair Information Practices* principles, we refer to the links in the footnotes.

Here, it will suffice to note that they all aim to addressing the inherent problem with computers: that by their very nature they facilitate many new uses of data, including personal data, without security and use restrictions being an inherent aspect of their specificity. In other words, the basic principles all seek to prevent abuses of personal data that the new technologies make all too easy unless checked. In that sense, they remain meaningful.

As set out concisely in the OECD Guidelines.

1980 OECD Principles

Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the previous principle] except:

a) with the consent of the data subject; or

b) by the authority of law.

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Note that the OECD Guidelines were revised in 2013 in the context of the creation of a wider OECD *Privacy Framework* that also includes new rules on privacy enforcement cooperation, that built on a 2007 recommendation on the issue, see:
https://www.oecd.org/sti/ieconomy/privacy.htm
But this does not affect the basic 1980s principles.

[42] United Nations, Guidelines for the Regulation of Computerized Personal Data Files, UNGA Res. 44/132, 44 UN GAOR Supp. (No. 49) at 211, UN Doc. A/44/49 (1989), available at:
https://www1.umn.edu/humanrts/instree/q2grcpd.htm
Note that this is the first instrument to recognise the need for independent data protection authorities.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

It is important to stress that the principles (in all of the instruments) should always be read and applied together: it is only then that they can provide serious protection against misuses or abuses of personal data such as errors in digitalised or stored data, collecting more data than necessary or keeping them for longer than necessary, using data for different purposes, stealing or disclosing data to others for illegal purposes, data losses, hacking, etc., etc.

1.2.3 The 1981 Council of Europe Data Protection Convention and its Additional Protocol

The first binding international instrument in the field of data protection was the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, better known as the Data Protection Convention (DPC) or "Convention No. 108" after its number in the European Treaties Series.[43] As a Council of Europe Convention (rather than a "European Convention"), the Data Protection Convention is open for ratification also by states that are not members of the Council of Europe, by invitation (Art. 23). To date (August 2018), the Convention has been ratified by all 47 Council of Europe Member States, and by six non-European countries (Uruguay [2013], Mauritius [2016], Senegal [2016], Tunisia [2017], Cabo Verde and Mexico [2018]).[44] Two further non-

[43] Full title: Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature in Strasbourg on 28 January 1981, CETS No. 108, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

[44] See: https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/108/signatures?p_auth=qsJbzlEi

European states have been invited to join the Convention: Argentina and Burkina Faso.[45] In 2001, the Convention was augmented by an Additional Protocol.[46]

The 1981 Convention and that Additional Protocol are briefly described below in the past tense because more recently, in 2018, they were more fundamentally amended ("modernised") in a further protocol, as discussed in section 1.3, below. However, it should be stressed that the revised ("modernised")Convention" will only apply to those state-parties that accede to it: for the others, the 1981 text remains the applicable one (read with the 2001 Additional Protocol as applicable).

As a binding international instrument, the 1981 Convention (unlike the earlier non-binding instruments) had to, and usefully did, include more precise, legal **definitions** of the main concepts in data protection law: "**personal data**", "**controller**" and "**processing**" (although in later binding instruments these needed, and were, expanded upon and added to) (Art. 2).

The main data protection principles discussed above – the **Collection Limitation Principle**, **Data Quality Principle**, **Purpose Specification Principle** and **Use Limitation Principle** – were set out in Article 5 of the 1981 Convention (without those terms being used: the Convention lists these principles together under the heading "*Quality of data*"). The **Data Security Principle** (referred to in the Convention as the *Security Safeguards Principle*) was spelled out in Article 7; and the **Openness- and Individual Participation Principles** were set out in Article 8 (under the heading "*Additional safeguards for the data subject*").[47]

The Convention added to these a special article on the processing of "**special categories of data**", i.e., "*personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life*" and "*personal data relating to criminal convictions*" (Art. 6). It stipulated that such data – commonly referred to as "**sensitive data**" – "*may not be processed automatically unless domestic law provides appropriate safeguards*".

NB: The need for special rules on certain types of data was hotly debated at the time. Some, including Simitis, felt that any data could be sensitive, depending on the context, while some of the listed data could be innocuous in other contexts. Others felt that only sensitive data needed to be regulated, because they were inherently dangerous and could lead to discrimination. In the end, the proposal made by Louis Joinet, the French representative and

---

45 *Idem*.

46 Full title: Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, opened for signature in Strasbourg on 8 November 2001, CETS No. 181, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626
The Additional Protocol has been ratified by 36 of the 47 Council of Europe Member States, and by six non-Member States (Cabo Verde, Mauritius, Mexico, Senegal, Tunisia and Uruguay). Burkina Faso has been invited to accede. See:
https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/181/signatures?p_auth=yDDCP83k

47 Because the application of the core principles constitutes the primary safeguards of individuals: the rights of data subjects are complementary to those, because they allow for more control by the individual, in individual cases.

chairman of the Council of Europe committee in charge of the drafting,[48] prevailed, and all personal data were regulated, with a higher level of protection for those sensitive data.

At the same time, the Convention allowed State-Parties to adopt **exceptions and restrictions** to most of the requirements of the Convention (but not to the data security requirements), to protect "***state security, public safety, the monetary interests of the state or the suppression of criminal offences***" or "***the data subject or the rights and freedoms of others***", provided that the derogation was "provided for by the ***law*** of the Party" and "constitutes a ***necessary****[and* ***proportionate****]*measure in a democratic society" to protect those interests (Art. 9(2)).[49]

Apart from giving legal effect to the core data protection principles (with the addition of the special rules on sensitive data) and data subject rights, the 1981 Convention also confirmed two of the other above-mentioned European **regulatory requirements**:

- It required state-parties to apply its provisions in **binding legal rules**. These could take the form of statute law, regulations or administrative provisions, and they could be supplemented by non-binding guidance or codes – but the main rules themselves had to take the form of "binding measures".[50]
- It required the state-parties to apply their laws broadly, **to (all) "automated personal data files and automatic processing of personal data in the public and private sectors"** (Art. 3(1)). In other words, at least in principle, it required the adoption of **"omnibus" laws**.[51]

However, the 1981 Convention did not yet require the state-parties to it to establish an independent **data protection authority**. It also did not yet address an issue that soon became prominent in the light of ever-increasing transborder data flows: **the need to restrict such transborder flows** in order to prevent circumvention of the substantive rules and negation of the crucial data subject rights, by imposing rules to ensure that protection would continue to be accorded also after the data left the territory of a state with proper data protection laws.

Rather, the 1981 Convention stipulated merely that state-parties:

> shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party (Art. 12(2)) – unless the state-party in question had adopted stricter rules for the relevant category of data, or the transfer to the other state-party was made with the intention to circumvent the law in the first state-party (Art. 12(3)).

---

[48] Louis Joinet was, until his retirement, a senior French judge who had been a member of the *ad hoc* commission for the drafting of the 1978 French data protection law before becoming the first director of the French DPA (the CNIL). He became a highly distinguished French representative at the UN Human Rights Committee and in that capacity was in charge of the drafting of the UN Guidelines (footnote 42, above). See: https://fr.wikipedia.org/wiki/Louis_Joinet
http://www.liberation.fr/societe/2013/12/18/louis-joinet-le-hessel-de-la-justice_967496

[49] In ECHR law, the requirement of proportionality is read into the expressly stipulated requirement of necessity (in a democratic society), whereas in EU law – in particular in the EU Charter of Fundamental Rights – the two concepts are dealt with as separate (though still closely-related) principles: cf. Art. 52 CFR.

[50] Explanatory Memorandum to the Council of Europe Convention, o.c. (footnote 19, above), para. 39.

[51] This is subject to the stipulation that any State-Party may declare "that it will not apply this convention to certain categories of automated personal data files" (Art. 3(2)(a)).

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

In other words, the 1981 Convention did not deal with the issue of personal data flowing to non-parties to the Convention.

Finally, it may be noted that the Convention only applied to "automated personal data files and automatic processing of personal data" (Art. 3(1), cf. also Art. 1). In other words, **manual files**, including "structured manual files", were not yet subject to its provisions (although State-Parties could choose to extend the application of the Convention to such files: Art. 3(2)(c)).

Two of the defects were corrected in the Additional Protocol regarding supervisory authorities and transborder data flows, adopted in 2001 (already mentioned),[52] which, as the title indicates, requires the establishment of **independent DPAs with powers of investigation and intervention, and to bring legal proceedings** (Art. 1) and the imposition of an **in-principle prohibition on the transfer of personal data to a country that does not ensure an "adequate level of protection"** (Art. 2). The Additional Protocol was adopted mainly to bring the regime in the Convention closer in line with the regime under the by then in force 1995 EC Data Protection Directive, discussed at 1.3, below.

Very recently, in May 2018, the 1981 Convention was further "**modernised**", to bring it into line with more recent EU data protection law and general (global) data protection developments, as further discussed at 1.4.3, below.

Within the Council of Europe, data protection issues are further addressed by a number of bodies including the Parliamentary Assembly of the Council of Europe (PACE), a Consultative Committee, known as "T-PD", established by Convention No. 108 – which has major responsibility for the daily monitoring of data protection-relevant developments and for elaborating draft sectoral and other guidelines and recommendations in this area – and the Council of Europe Committee of Ministers (COM or CM), which then adopts in particular those proposals. Between them, they have issued many opinions, recommendations and studies in the area – always with reference to the Convention.[53]

In addition, there is an interplay between the Data Protection Convention and the European Convention on Human Rights, with the European Court of Human Rights increasingly taking note of the Data Protection Convention and the above-mentioned kinds of documents in its own interpretation of Article 8 of the Human Rights Convention (which guarantees the right to private life); while PACE, the Consultative Committee and the Committee of Ministers in turn draw on the case-law of the Court in their work in this area.[54]

---

[52] See footnote 46, above.

[53] See:
http://website-pace.net/en_GB/web/apce/documents (PACE documents) Note that these cover many more issues than just data protection – but they can be searched under the term "data protection".
https://www.coe.int/t/dghl/standardsetting/dataprotection/Documents_TPD_en.asp (T-PD documents);
https://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp (COM documents relating to data protection).

[54] See the Council of Europe Factsheet – personal data protection (footnote 13, above) and *Annex 1 – Jurisprudence* to a working document by the EU's "Article 29 Working Party", Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (WP237), adopted on 13 April 2016, which lists 15 important ECtHR judgments relevant to data protection (and five CJEU ones), available at:
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf

1.3 European Community data protection law in the 1990s and early-2000s

1.3.1 Data protection in the European Community

Background

For some time, it was felt by the European Community (as the EU was then called)[55] that the 1981 Council of Europe Data Protection Convention accorded sufficient protection in this field. However, by the end of that decade, it had become clear that the Convention had not led to broad, or broadly harmonised protection of personal data in the Community: it had, by September 1990, only been ratified by seven EC Member States (of which one had actually not yet adopted the relevant legislation), and the laws in those Member States differed considerably in important respects.[56] At the time, Italy only had a data protection law in relation to workers, Spain had no omnibus law even though it provided for data protection as a fundamental right in its Constitution, etc.

This diversity ran counter to the aim of the European Community at the time, to harmonise all manner of rules and laws in order to facilitate the opening of the internal market, with its proposed free circulation of goods, services, capital and persons.More specifically, during the 1989 international conference of data protection authorities in Berlin, the assembled representatives were informed by the European Commission that the rules for the sector of telecommunications were to be harmonised. This showed that it had become crucial to also have well-applied, strong data protection laws in place in all the Member States.[57]

Consequently, the following year, in September 1990, in response to this appeal by the European DPAs, the European Commission therefore put forward an ambitious set of proposals, aimed at protecting personal data throughout the First Pillar of the EC.[58] The

---

[55] At the time of the introduction of the package of Commission proposals discussed in this section (September 1990), the Commission was still formally the "Commission of the European Communities" (plural). The term "European Community" (singular) only came to be applied in 1992, under the Maastricht Treaty, until the coming into effect of the Lisbon Treaty in 2009. However, for simplicity sake, we will generally refer to the European Community in the present section, and to the European Union in the next one, section 1.4, and in Parts Two and Three.

[56] Commission of the European Communities, Communication on the protection of individuals in relation to the processing of personal data in the Community and information security, COM(90) 314 final – SYN287 and 288, Brussels, 13 September 1990, *Introduction*. The full document is available online from the excellent archive of the Cambridge University-based Centre for Intellectual Property and Information Law, at: https://resources.law.cam.ac.uk/cipil/travaux/data_protection/3%2013%20September%201990%20Communication.pdf.
See in particular paras. 6 – 8.

[57] At the Berlin Conference, Spiros Simitis, the Data Protection Commissioner for the German Land of Hessen (and the initiator of the first data protection law in the world in that state) publicly called on Jacques Fauvet, the then chairman of the French data protection authority, the CNIL (and previously the head of the newspaper "*Le Monde*"), to write to his long friend Jacques Delors, then President of the European Commission at that time, to take an initiative to harmonise data protection laws within the EC.

[58] The Treaty on European Union, signed in Maastricht on 7 February 1992 (the "Maastricht Treaty"), provided for a three-pillar structure under a single pediment. The First Pillar was made up of the original European Economic Community (EEC), European Coal and Steel Community (ECSC) and European Atomic Energy Community (EAEC) (although each retained their own legal personality) and subsequently covered the Single Market which was created in 1993. The Second and Third Pillars covered, respectively, the Common Foreign and Security Policy (CFSP) and cooperation in the fields of Justice and Home Affairs (JHA). The pillars were formally abolished by the Lisbon Treaty, but separate instruments are still issued for the distinct areas (cf. the discussion of the scope of the GDPR in Part Two, section 2.3, below). See the University of

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

package included proposals for two First Pillar directives, i.e.:[59]

- a **general EC directive** "*concerning the protection of individuals in relation to the processing of personal data*" – which after a protracted legislative process became the main EC Data Protection Directive, Directive 95/46/EC, discussed below, at 1.3.2; and
- a proposed further, **subsidiaryEC directive** "*concerning the protection of personal data in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks*" – which became the Telecommunications Data Protection Directive, Directive 97/66/EC, adopted in December 1997, since replaced by Directive 2002/58/EC, the so-called "e-Privacy Directive, discussed below, at 1.3.3;

Before discussing these two directives, it is important to note the nature and inherent limitations of such instruments.

Nature and limitations of EC directives

In discussing the main EU data protection instruments, and in particular the two above-

---

Luxembourg's CVCE research centre's website on Historical events in the European integration process (1945 – 2014), in particular the page on "*The first pillar of the European Union*: https://www.cvce.eu/en/education/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/4ee15c10-5bdf-43b1-9b5f-2553d5a41274

The 1995 Data Protection Directive (and the other directives discussed in the present section) was (and were) all issued at the time when the First Pillar was still in place, and were issued for that pillar only. Data protection measures in the other two pillars are briefly noted in sub-sections 1.3.4 and 1.3.5, below, and data protection rules for the EU institutions themselves are briefly discussed in sub-section 1.3.6.

[59] Commission of the European Communities, Communication on the protection of individuals in relation to the processing of personal data in the Community and information security (footnote 56, above). The package contained four further proposals, i.e.:

- a draft **resolution** of the representatives of the Member States which would have extended the application of the principles contained in the general directive to files held by public authorities to which the main Data Protection Directive would not, as such, apply – which was never adopted as such but can be seen as the genesis of the data protection rules relating to law enforcement and judicial matters, most recently culminating in the Law Enforcement Data Protection Directive (Directive (EU) 2016/680 (not discussed in this handbook: see the Note in the box "*About this handbook*" on p. 1, above);
- a draft Commission **declaration** on the application of the data protection standards set by the main Data Protection Directive to files held by the Community institutions themselves – which ultimately led to Regulation (EC) 45/2001 (*idem*);
- a **recommendation for a Council decision** on the accession of the European Community to the Council of Europe Convention on Data Protection – which to date has not happened because the EU, not being a Member State, cannot accede to the Convention – but this is being remedied in the "Modernised" Council of Europe Data Protection Convention, discussed below, at 1.4.3; and
- a **proposal for a Council decision** on the adoption of an action plan on information security – which led to extensive action in that field by the EU, including the establishment, in 2004, of the European Union Agency for Network and Information Security, ENISA, and the adoption of an elaborate information- and cybersecurity strategy, which are not discussed further in this handbook, but information on which can be found here:
  https://www.enisa.europa.eu/about-enisa
  https://ec.europa.eu/digital-single-market/en/cyber-security

For the separate proposals listed in the Commission Communication (and further documents relating to the legislative process), follow the links on this page:
https://www.cipil.law.cam.ac.uk/projectseuropean-travaux/data-protection-directive

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

mentioned data protection directives, three matters should be borne in mind. First of all, any EU (or previously: EC) legal instrument is, by its very nature, limited to matters within the scope of EU (or previously: EC) law. Certain matters, most notably the activities of the Member States in relation to **national security**, are (almost) entirely outside of the scope of EU (or previously: EC) law,[60] and no EU (or EC) legal instruments (including those directives – or indeed the GDPR, or any future EU data protection rules, in whatever form) are therefore applicable to such activities. This is expressly reaffirmed in the directives (and the GDPR): see Article 3(2) of the 1995 Data Protection Directive and Article 1(3) of the e-Privacy Directive (and Art. 2(2)(a) GDPR).[61]

Secondly, the EC directives discussed below were, as EC directives, limited to matters within the so-called**First Pillar**,[62] and by their very nature of EC directives did not apply to Second- or Third Pillar activities, for which separate data protection instruments have been drafted that are briefly mentioned in sections 1.3.4 and 1.3.5, below, but not further discussed in this first edition of the handbook. Suffice it to note that *any passing on or making available of personal data* by entities subject to the directives (including both private- sector entities and public bodies that are carrying out activities subject to First Pillar (EC) law), to any law enforcement or national security agency was (and in the case of the e-Privacy Directive still is) subject to those instruments (because such disclosures constituted "processing" in terms of those directives, by those entities), even if the *obtaining (receiving) and further processing* of the disclosed data was either subject to other instruments (including, in relation to law enforcement in particular, until recently, Council Framework Decision 2008/977/JHA and, now, the 2016 Law Enforcement Data Protection Directive), or not subject to EU (or EC) law at all (i.e., if it was done by national security agencies).[63]

Third, a directive, by definition, does not apply directly in the legal orders of the Member States: it does not have "direct effect". Rather, its provisions must be "**transposed**" into national law by the Member States – and in this, the Member States were (and still are) often granted considerable **discretion**. This was certainly the case in relation to the two directives discussed below – and as will be noted in Part Two, this led to considerable divergences between the national laws of the Member States implementing ("transposing") those directives; that indeed was one of the main reasons for choosing the form of a (directly applicable) regulation for the successor to the 1995 Data Protection Directive, the GDPR (even though, as we shall see in that part, the Regulation still also allows for different

---

60 We say "(almost) wholly" for two reasons. First of all, it is becoming increasingly difficult, especially in relation to terrorism (itself a rather ill-defined concept) to distinguish actions by states in relation to their national security from actions taken under criminal law or the law relating to protection of "international security", "public security" or "public order" – all of which are matters that are, to a greater or lesser degree, now at least partially subject to EU law. Secondly, even if actions by Member States' agencies responsible for national security are outside the scope of EU law, closely related activities by law enforcement agencies and private entities (e.g., collection and disclosure of data by banks under money laundering legislation, or the collection and disclosure of Passenger Name Records by airlines to Member States' agencies) are often subject to EU law (in particular EU data protection law). Cf. the second point in the text.

61 On the limitations on the scope of the EU General Data Protection Regulation, see Part Two, section 2.3, *Key elements of the GDPR*, in particular sub-section 2.3.1, General provisions.

62 See footnote 67, below.

63 On the similar issues raised in relation to the EU General Data Protection Regulation, see Part Two, in particular section 2.2, *Status and approach of the GDPR: harmonisation with specifications at the national level*.

implementation in many respects.[64]

1.3.2 The main 1995 EC Data Protection Directive

General

As noted above, in the early-1990s, the Commission of the European Communities (as it was then known)[65]was faced with a dilemma. On the one hand, data protection was increasingly recognised as an EU-constitutionally-protected right, and required restrictions on the use and flows of personal data.[66] On the other hand, the development of the **internal market**, in the so-called "First Pillar" of the Community,[67] required the free flow of data, including personal data, related to commercial transactions. In order to square this circle, the Commission proposed that for this First Pillar, two directives be adopted. In this section, we will discuss the main directive, Directive 95/46/EC.[68]

Aim and purpose of the 1995 Data Protection Directive:

In recognition of the above dilemma, the European Community gave the directive two

---

[64] See Part Two, in particular section 2.2, *Status and approach of the GDPR: harmonisation with flexibility*.

[65] See footnote 67, below.

[66] Data protection is now expressly recognised as a *sui generis* right in Article 8 of the EU Charter of Fundamental Rights (CFR), distinct from (although of course closely related to) the right to private and family life and privacy, protection by Article 7. The CFR was only proclaimed in 2000 but did not gain full legal effect until the entry into force of the Lisbon Treaty on 1 December 2009. See:
https://en.wikipedia.org/wiki/Charter_of_Fundamental_Rights_of_the_European_Union
In other words, the Charter did not yet have full legal effect at the time the directives were proposed. However, even before the Charter was drafted or given legal effect, fundamental rights were already given quasi-constitutional status in the European Communities, see: Francesca Ferraro and Jesús Carmona, Fundamental Rights in the European Union – The role of the Charter after the Lisbon Treaty, European Parliament Research Service, Brussels, March 2015,section 2*: EU Fundamental rights prior to the Lisbon Treaty*, available at:
http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/554168/EPRS_IDA(2015)554168_EN.pdf
The drafters of the 1995 Data Protection Directive therefore still rightly placed personal data protection as a fundamental right at the foundation of the proposed instrument.

[67] The Treaty on European Union, signed in Maastricht on 7 February 1992 (the "Maastricht Treaty"), provided for a three-pillar structure under a single pediment. The First Pillar was made up of the original European Economic Community (EEC), European Coal and Steel Community (ECSC) and European Atomic Energy Community (EAEC) (although each retained their own legal personality). The Second and Third Pillars covered, respectively, the Common Foreign and Security Policy (CFSP) and cooperation in the fields of Justice and Home Affairs (JHA). The pillars were formally abolished by the Lisbon Treaty, but separate instruments are still issued for the distinct areas (cf. the discussion of the scope of the GDPR in Part Two, section 2.3, below). See the University of Luxembourg's CVCE research centre's website on Historical events in the European integration process (1945 – 2014), in particular the page on "*The first pillar of the European Union*:
https://www.cvce.eu/en/education/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/4ee15c10-5bdf-43b1-9b5f-2553d5a41274
See also the Wikipedia entry on *The Three Pillars of the European Union*, available at:
https://en.wikipedia.org/wiki/Three_pillars_of_the_European_Union
(With a very useful timeline illustrating the developments.)
The 1995 Data Protection Directive (and the other directives discussed in the present section) was (and were) all issued at the time when the First Pillar was still in place, and were issued for that pillar only.

[68] Full title: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281, 23.11.1995, pp. 31 – 50, available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

linked aims, i.e.: providing for **a high level of data protection** throughout the then "First Pillar" of the Community ("high level" because the directive sought to protect human rights), as a *conditio sine qua non* for the **free flow of personal data** within that pillar's main element, the then-emerging **internal market** (see Article 1 of the Directive and Recitals 10 and, especially, 11).

Key features of the 1995 Data Protection Directive:

Below are set out the **key features** of the 1995 Data Protection Directive, compared to the 1981 Convention (NB: New features or features containing important new elements are marked *NEW – although it should be noted that often they expand on suggestions already made or hinted at in the recitals to the Convention). The description of these key features of the 1995 Directive is meant to provide an overview of some fundamental components of the data protection approach in the EU, which have been fully re-affirmed in the 2016 General Data Protection Regulation and are accordingly explained here whilst the main new features introduced via the Regulation will be highlighted in Part Two. The most important innovations were the requirement of independent data protection authorities and measures to ensure continued protection of data transferred to third (i.e., non-EU/EEA) countries.

*NEW Definitions:

The Directive expanded on the core **definitions** in the 1981 Convention and added new ones. Specifically, it clarified (within the definition of "personal data") when individuals should be deemed to be "***identifiable***" (by "anyone"), and (in a separate definition) when a manual dataset should be deemed to be sufficiently "***structured***" to be subject to the Directive. "[Structured] manual files" were included in the scope of the Directive to avoid circumvention of its rules by the use of such files.

The Directive set out ***a somewhat modified definition of "controller"***, and added ***an all-encompassing definition of "processing of personal data"*** and definitions of the concepts of "***processor***", "***third party***" and "***recipient***". It also added a definition of "***the data subject's consent***" that in effect set out the conditions that should be met before any claimed consent could be deemed valid: consent, to be valid, had to be "***freely given specific and informed***" and in some way ***expressed*** (Art. 2(h)).[69]

Where the 1981 Convention had four definitions, the Directive provided eight (or nine, if one counts the definition of an "identifiable person" within the definition of "personal data" as a separate one).

Data protection principles:

The Directive largely repeated the **data protection principles** from the 1981 Convention, but with some **clarifications**, including that the ***purpose*** for which personal data are to be processed should not only be "*specified*" and "*legitimate*" (as already stipulated in Article 5(b) of the Convention), but also "*explicit*" (Art. 6(1)(b)), and as concerns "*[f]urther processing of data for historical, statistical or scientific purposes*" (See Art. 6(1)(c) and (e)).

[69] The consent had to take the form of a "freely given specific and informed **indication of his wishesby which the data subject signifies his agreement** to personal data relating to him being processed", to quote the full text.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

*NEW Legal bases for processing

A major new feature of the 1995 Directive was that, in order to achieve greater harmonisation between the laws of the Member States, it laid down, in Article 7, **an exhaustive list of "criteria for making data processing legitimate"** – what were later to be called the **"legal bases" for processing of personal data**. Under the Directive, processing of (non-sensitive) personal data was only allowed if (in summary):

(a) the data subject had ***unambiguously*** given his **consent** (which of course also had to be "***free, specific and informed***" and ***expressed***: Art. 2(h), noted above); or

(b) processing was ***necessary*** for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (e.g., for a credit check); or

(c) processing was ***necessary*** for compliance with a **legal obligation** to which the controller is subject; or

(d) processing was ***necessary*** in order to protect the **vital interests of the data subject**; or

(e) processing was ***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; or

(f) processing was ***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 were overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1). [the so-called "legitimate interests" or "balance" criterion/legal basis].

Put simply: for most cases, processing of non-sensitive personal data was allowed, either on the basis of a law, or for a contract, or with the consent of the data subject, or on the basis that it served a legitimate interest of the controller that was not out-weighed by the interests or fundamental rights and freedoms of the data subjects.

No such list was contained in the 1981 Data Protection Convention.

*NEW Specific rules on the processing of sensitive data

The 1995 Directive listed largely the same **main** "**special categories of data**" – usually referred to as "**sensitive data**" – as were set out in the 1981 Convention, with minor changes, i.e.:[70]

> personal data revealing racial *or ethnic* origin, political opinions, religious or *philosophical* beliefs, *trade-union membership*, and … data concerning health or sex life

However, rather than merely stipulating that such data "*should not be processed automatically unless domestic law provides appropriate safeguards*" (Council of Europe Convention, Art. 6), the Directive, in Article 8(1), laid down an **in-principle prohibition** on the processing of such sensitive data, subject to a limited number of **exceptions**. The main exceptions in effect amounted to **especially restrictive legal bases** for the processing of

[70] The 1981 Convention did not include the reference to "ethnic" data, referred to "religious or other beliefs" (rather than "religious or philosophical beliefs"), and did not include trade union membership.

sensitive data. They were (again in summary):

- processing on the basis of the not just free, specific and informed, but also***explicit*** **consent** of the data subject except where a national law would prohibit the processing of such data even with the consent of the data subject in particular circumstances (art. 8(2)(a));
- processing that is ***necessary*** to meet obligations and rights of the controller under **employment law** (provided national law provides for "adequate safeguard") (Art. 8(2)(b));
- processing that is ***necessary*** to protect the **vital interests** of the data subject or another person where the data subject is physically or legally incapable of giving his consent (Art. 8(2)(c));
- processing "carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other **non-profit-seeking body with a political, philosophical, religious or trade-union aim** and on condition that the processing relates solely to the ***members*** of the body or to ***persons who have regular contact with it*** in connection with its purposes and that' the data are ***not disclosed to a third party*** without the consent of the data subjects" (Art. 8(2)(d));
- processing of (sensitive) personal data "which are **manifestly made public by the data subject**" (Art. 8(2)(e), first sub-sentence); and
- processing of (sensitive) personal data which is "necessary for the establishment, exercise or defence of **legal claims**" (Art. 8(2)(e), second sub-sentence).

Notably, the list did not include a "**legitimate interest**" or "**balance**" criterion: the processing of sensitive data could, already under the Directive, *in principle* not be processed on the basis that it was in the legitimate interests of the controller or a third party, which were not outweighed by the fundamental rights interests of the data subject.

However, the Directive also stipulated that the in-principle prohibition of the processing of sensitive data (note: of any type of sensitive data) did not apply "*where processing of the data is* ***required*** *for the purposes of* ***preventive medicine, medical diagnosis****, the provision of* ***care*** *or* ***treatment*** *or the* ***management of health-care services***", provided this was done under a relevant obligation of secrecy (Art. 8(3)). Note that this applies to any type of sensitive data – but of course, such data may still only be used for such purposes when relevant (e.g., information on ethnic origin may be relevant in relation to certain diseases such as sickle-cell anaemia; and a person's religious beliefs may be relevant to certain treatments, such as blood transfusion for Jehovah's Witnesses).

Moreover, although the above rules were, as such, strict, the Directive also contained a much more broadly-phrased clause (Art. 8(4)) that allowed Member States to grant **additional exceptions** – i.e., to allow the processing of (any type of) sensitive data other than on the basis of the grounds listed in Article 8(2) – either by law, or by decision of their national supervisory authority (data protection authority, "***for reasons of substantial public interest***", provided this was made subject to "***suitable safeguards***" – to be defined by the Member State.

The Directive also set out a somewhat more restrictive approach to the processing of **personal data relating tocriminal convictions** (Art. 8(5)) and of **national identification numbers or other "identifier[s] of general application"** (Art. 8(7)) – but left the details of the regulation of such processing to the Member States.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Similarly, while it was more emphatic than the 1981 Convention about the need to **balance data protection and freedom of expression and information**, it left the specific striking of this balance also to the Member States (Art. 9).

*NEW Informing data subjects

The 1981 Data Protection Convention only required some general transparency about "*the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file*" (Art. 8(a)).

By contrast, Articles 10 and 11 of the 1995 Data Protection Directive set out in some detail the **information that should be provided by any controller to the data subjects**, *of the controller's own motion*, when, respectively, the personal data were collected from them, or from a third party. The details to be provided included, in both cases, the ***identity of the controller*** and the ***purposes of the processing***. ***Further information*** (including information on the data to be collected being mandatory or not, information on any disclosures of the data) had to be provided insofar as necessary to guarantee fair processing (see Arts. 10(c) and 11(1)(c)).

*NEW Data subject's rights

The 1981 Data Protection Convention already required that data subjects should be given the right to obtain **access** to their data on request, at reasonable intervals; the right to **rectification or erasure** of data that were incorrect or processed in violation of the data protection principles; and a right to a **remedy** if the exercise of these rights was not complied with (Art. 8(b) – (d)).

The Directive confirmed the first two rights, but added **important further detail**. It confirmed that the **right of access** included the right to have the data "communicated" to the data subject (which was already stipulated in the Convention), but added that this had to be "*in intelligible form*" and that "*any available information as to [the data's]* ***source***" should also be provided (Art. 12(a), second bullet-point). It added "***blocking***" as an option aside from rectification and erasure (albeit without defining the concept)[71] (Art. 12(b)); and it stipulated that any rectifications, blockings or erasures should be brought to the attention of ***third parties*** to whom the data had been disclosed (Art. 12(c)).

It also introduced new rights: a **general right toobject** to processing on "compelling legitimate grounds", "at least" in relation to processing for a task carried out in the public interest or in the exercise of official authority, or based on the "legitimate interest"/"balance" criterion – with such an objection having to be complied with if it was "justified" (Art. 14(a)); a more specific and stronger **right to object to processing of one's data for direct marketing purposes** (in those days, mainly be means of direct mail – this is before the birth of the Internet and "spam" emailing) – which always had to be respected, without the data subject having to provide any justification (Art. 14(b)); and a **right not to be subject to a fully-automated decision based on profiling**[72] that had legal or other significant effects (subject to important but strictly qualified ***exceptions***) (Art. 15). In that

[71] The corresponding concept of "**restriction of processing**" is defined in the GDPR as "*the marking of stored personal data with the aim of limiting their processing in the future*" (Art. 4(3) GDPR).

[72] In full: "*a decision which produces legal effects concerning [the data subject] or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.*" The provision was taken directly from the French Data Protection Law of 1978, Articles 2 and 3.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

last regard, it is important to note that Article 12(a), third bullet-point, stipulated that data subjects also had a **new** right to obtain (in the context of an access request) **information on the "logic"** involved in any automated processing of data concerning them, "at least" in the case of such fully-automated decisions based on profiling.

These rights in the 1995 Directive, which are carried over and further strengthened in the GDPR, are becoming of ever-greater importance in relation to the taking of decisions based on "Artificial Intelligence".

*NEW Confidentiality and security of data

The 1981 Convention simply stipulated that "appropriate security measures" had to be taken to protect personal data against "accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination" (Art. 7).

The Directive considerably expanded on this by imposing, first of all, a **duty of confidentiality** on anyone involved in the processing of personal data (Art. 16), and then stipulating that the controller was required to implement "*appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing*" (Art. 17(1), with further detail). This latter provision was taken from the 1977 Federal German Data Protection Law.

It also laid down important new requirements for when a controller engaged a processor to process data on his (the controller's) behalf, including a requirement of "*sufficient guarantees*" in respect of security and confidentiality, and a requirement of a detailed written contract between the controller and the processor (Art. 17(2) – (4)).

*NEW Restrictions on transborder data transfers

As noted at 1.2.3, above, the 1981 Convention, as originally adopted, did not require the State-Parties to adopt a **prohibition of exports of personal data from their territory to a state that did not provide similar protection**. It dealt with only flows on personal data among parties to the convention. The introduction of such a prohibition (subject to limited exceptions) – which derived from French and Danish law and experience – was therefore another important new feature of the 1995 Directive.

Specifically, it stipulated that personal data subject to the Directive could in principle only be transferred to third countries that ensured a level of protection that could be deemed "**adequate**" in terms of the Directive (Art. 25(1)); and that it would be up to the European Commission to determine (by means of what came to be called an "**adequacy decision**") whether that was the case in respect of any specific third country (Art. 25(2)).[73] The Commission went on to determine "adequacy" not only in relation to third countries as a whole, but also to **sectors** in particular countries (e.g., initially, the regime for public-sector bodies in Canada) and indeed for special **schemes** established in certain countries (i.e., the

[73] The term "adequate protection" was chosen because the term "equivalent" was reserved in EC (then EU) law to relations between rules among Member States while, based on international law, it would have been "equivalent in effect". But In its judgment in *Maximillian Schrems v. Data Protection Commissioner*, CJEU judgment in Case C-362/14, 6 December 2015, the Court held that the term "adequate protection" should be read as in effect requiring "essentially equivalent" protection in the third state: see para. 96 of the judgment – but that was of course many years after the 1995 Directive (or indeed the 2001 Additional Protocol to the 1981 Convention, noted later in the text) were adopted.

"*Safe Harbor*" regime established by the USA, since replaced by the "*Privacy Shield*" regime).

The in-principle prohibition on transfer to countries (or sectors in countries) without adequate protection was subject to a limited number of **exceptions** set out in Article 26(1) of the Directive, most of which were similar to the legal grounds for processing generally, i.e. (in summary):

(a) the data subject had ***unambiguously*** given his **consent** to the transfer (which of course also had to be "***free, specific and informed***" and ***expressed***: Art. 2(h), noted earlier); or
(b) the transfer was ***necessary*** for the performance of a **contract** between the controller and the data subject, or in order to take steps at the request of the data subject prior to entering into a contract (e.g., for a credit check);
(c) the transfer was ***necessary*** for the conclusion or performance of a **contract** between the controller and a third party, concluded in the interest of the data subject (e.g., a hotel booking);
(d) the transfer is ***necessary*** or ***legally required*** on **important public interest** grounds, or for the establishment, exercise or defence of **legal claims**;
(e) the transfer is ***necessary*** to protect the **vital interests of the data subject**; or
(f) the transfer is made from **a register open to the public** (subject to any conditions that apply to access to the register generally)

In addition, Member States were allowed to **authorise** transfers where the controller adduced "***adequate safeguards***" for the protection of the data protection interests and rights of the data subjects (Art. 26(2)) – e.g., in the form of ***ad hoc data transfer clauses***; and the Commission was **authorised** to approve certain "***standard contractual clauses***" for data transfers, that would ensure such protection (Art. 26(4)).

A number of DPAs, and in their wake, the WP29, also looked at safeguards contained in so-called ***Binding Corporate Rules*** (BCRs), i.e., in rules drawn up by international companies or groups of companies that regulated the internal uses and flows of personal data within such companies or groups.[74] In spite of hesitation on the part of some other DPAs, the idea was formally included in the GDPR (as noted in Part Two).

---

[74] The WP29 addressed BCRs in a whole range of working documents and recommendations including:
- Working document: 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, adopted by the Article 29 Working Party on 3 June 2003 (WP74);
- Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, adopted by the Article 29 Working Party on 3 June 2003 (WP108);
- Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data, adopted by the Article 29 Working Party on 10 January 2007 (WP133);
- Working document setting up a table with the elements and principles to be found in Binding Corporate Rules, adopted by the Article 29 Working Party on 24 June 2008 (WP153);
- Working document setting up a framework for the structure of Binding Corporate Rules, adopted by the Article 29 Working Party on 24 June 2008 (WP154);
- Working document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules, adopted by the Article 29 Working Party on 24 June 2008, as last revised and adopted on 8 April 2009 (WP155);
- Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, adopted on 6 June 2012 (WP195).

See also:
- Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents, adopted on 27 February 2014 (WP212).

The restrictions on transfers of personal data to third countries without adequate protection stimulated action outside Europe. In particular, the Spanish and French DPAs used it to promote the adoption of appropriate laws in their respective global language zones, i.e., respectively, Latin America and French-speaking countries, especially in Africa.

NB: As noted at 1.2.3, above, an "adequacy" requirement for data transfers was introduced for the 1981 Convention in the 2001 Additional Protocol to that Convention, with the aim of bringing the Convention regime in this respect in line with the regime under the 1995 EC Directive (see Art. 2(1) AP) – although that of course only applies to those State-Parties to the original Convention that also acceded to the Protocol.[75]

*NEW Codes of conduct (and certifications)

Another new feature introduced by the Directive was its reference to **codes of conduct** as a means of "*contribut[ing] to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors*" (art. 27(1)) – although it only went as far as to "encourage" such codes (*idem*); requiring Member States to make provision for the assessment of ***draft national codes*** (Art. 27(2)); and itself making provision for the Article 29 Working Party (WP29, discussed below under that heading) to similarly assess ***draft Community-wide codes*** (Art. 27(3)).

In practice, only a very few such codes have been approved or even submitted for approval. The first draft of the European direct marketing association (FEDMA)'s European Code of Practice for the Use of Personal Data in Direct Marketing was submitted to the WP29 in 1998, but the final version was only approved in 2003.[76] A draft Code of Conduct for Cloud Service Providers, drawn up by an industry working group set up in 2013 and actually jointly chaired by two EU Directorate-Generals (DG connect and DG Justice) was submitted to the WP29 in January 2015, but was not approved by the WP29 in its opinion on the draft, and remains a "work in progress".[77]

Although not expressly mentioned in the Directive, the European Commission also encouraged the establishment of certification schemes.[78] It provided initial financing to a

---

[75] See footnote 46, above. Note that it is not clear whether the term "adequate" in this article in the Protocol can or should be interpreted in line with the judgment in *Schrems* (footnote 73, above) – and thus whether the AP actually achieved this aim.

[76] Text of the Code:
https://www.fedma.org/wp-content/uploads/2017/06/FEDMACodeEN.pdf
The Article 29 Working Party Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing, endorsing the code (WP77, adopted on 13 June 2003), is available at:
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp77_en.pdf

[77] See:
https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers
(19 July 2013 - general background and background documents)
https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers
(12 October 2015 - latest available information on this site)
Article 29 Working Party, Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing (WP232, adopted on 22 September 2015), available at:
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf
For further details and views in the light of the GDPR, see the letter from the WP29 to Cloud Infrastructure Services Providers in Europe of 6 February 2018, available at:
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615033

[78] When the Internet began to emerge in the wider world in the early 1990s, the French DPA suggested to the other EU DPAs and the European Commission that certification schemes could be a very efficient means of dealing with online services established outside Europe, but nothing was done at that time.

group of DPAs and experts led by the Schleswig-Holstein DPA for the establishment of **a pan-EU certification scheme, the *European Privacy Seal* (EuroPriSe)**, under which products and services that involve the use of personal data can be evaluated and, if assessed to be in conformity with the Directive (and where appropriate other EU data protection instruments such as the e-Privacy Directive, discussed under the next heading), granted a certificate confirming such conformity (although, since there is no formal basis for the scheme in the 1995 Directive, those certifications of course do not have legal force).[79]

*NEW Rules on "applicable law"

As should be clear from the various entries under different headings, above, under the Directive Member States had considerable discretion in determining the precise way in which they wanted to "transpose" the provisions of the Directive; many of those provisions left it to the Member States to adopt such rules as they deemed appropriate for particular contexts. This resulted in a serious lack of harmonisation[80] – and was one of the main reasons why the form of a regulation was chosen for the instruments to succeed the Directive.[81]

The difficulties caused by these divergences were to some extent alleviated by a crucial provision in the 1995 Data Protection Directive, on "applicable law". This provision (Art. 4) effectively laid down three different rules for the private sector:

(1) controllers that were established in only one Member State had to comply with the data protection law of that Member State in relation to any processing that they controlled and that was "carried out in the context of the activities of an establishment of [that] controller" (Art. 4(1)(a), first sub-sentence);

(2) controllers that were established in more then one Member State [read: had establishments in more than one Member State] had to ensure "that each of these establishments complies with the obligations laid down by the national law applicable" (which need not be the country of establishment of the establishment in question) (Art. 4(1)(a), second sub-sentence);

(3) controllers that were not established in the Community (EU) had to comply with the laws of any Member State on the territory of which they "made use of equipment, automated or otherwise" (Art. 4(12)(c)); and such controllers had to "designate a representative" in that territory (Art. 4(2)).[82]

---

79 See:
https://www.european-privacy-seal.eu/EPS-en/about-europrise

80 See the EU-commissioned study by Douwe Korff, Report on an EU study on the implementation of the [1995] data protection directive, 2002, available at:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667 –

81 See Part Two, section 2.1 and the text under the first sub-heading, "*A regulation …*" in section 2.2, below.

82 The application of this third rule was complicated by the use of different words in different (but all legally equally authentic) language versions: The original draft of the directive was in French, and used the term *moyens* – "means" in English. The word used in the other official Latin-based languages was the linguistic equivalent, all also meaning "means". The official German language version also used the same word, *Mittel*. However, the English text referred to the use of "*equipment*", and the Dutch language version also followed this (*middelen*). This led the UK and the Netherlands to limit the application of the rule to situations in which the non-EU/EEA controller *owned* a local piece of equipment in the EU/EEA, whereas other countries held that even the presence of a smartphone in the EU/EEA sufficed to make any controller "using" such a device to transit data subject to the Directive. Cf. the discussion of "applicable law" in relation to the e-Privacy Directive in section 1.3.3, below.

It is worth noting that these rules not only allowed Member States to protect the data protection rights of their **citizens** from violations by actors outside their territory or the EU. Rather, under all three rules, **data on all individuals** ("natural persons") processed by relevant controllers had to be protected, ***irrespective of whether the data subjects were in the EU or not, and irrespective of whether they were EU nationals or residents or not*** – in line with the principle of *universality of human rights*.[83]

These rules were difficult to apply in practice (in particular in relation to non-EU/EEA-based controllers),[84] but they provided at least some guidance on how to deal with different laws in different Member States that could in theory be applicable to any particular transnational personal data processing operation. No such a provision aimed at avoiding "conflicts of law" was contained in the 1981 Data Protection Convention.

As concerns the public sector, the determination of the applicable law was in practice more straightforward: all public authorities and bodies, including diplomatic institutions, were subject only to the data protection law (or laws) of their own Member State.

*NEW Supervisory authorities

Another major novelty of the 1995 Directive, compared to the 1981 Convention,[85] was the requirement that all Member States had to appoint:

> one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive
>
> (Art. 28(1), first sentence)

In order to be effective, these "**supervisory authorities**" – in practice more commonly referred to as ***data protection authorities*** or ***DPAs*** – (of which there were several in federal Member States), had to be granted extensive powers of ***investigation***, ***intervention*** and ***direction*** (including powers to order the blocking, erasure or destruction of data, or to ban processing) (Art. 28(3), first and second bullet-point), and had to be able to "*act with complete independence in exercising the functions entrusted to them*" (Art. 28(1), second sentence). The requirement of independence is also a requirement of democracy and the rule of law. Since the requirements of independence were not spelled out in the directive, the Commission had to resort to court actions against several Member States to have the matter clarified. The results of these court cases are reflected in the much more elaborate provisions in the GDPR in that regard.

They had to be ***consulted*** by the authorities when they drew up data protection-related

---

83 See Douwe Korff, Maintaining Trust in a Digital Connected Society, report written for the International Telecommunications Union (ITU), May 2016, section 2.3, *Universality of human rights*, available here: http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/ITU_MaintainingTrust_GSR16.pdf

84 See: Douwe Korff, *Der EG-Richtlinienentwurfüber Datenschutz und "anwendbaresRecht"*, in: Recht der Datenverarbeitung, Year 10 (1994), Vol. No. 5- 6, p. 209 ff; *The question of "applicable law"*, in: Compliance Guide 3 – Interim report (part of the New UK Data Protection Act 1998 Information & Compliance Programme), Privacy Laws & Business, November 1999.

85 It was already provided for in the non-binding UN Guidelines adopted in 1990 (see footnote 42, above). Also, as noted at 1.2.3, above, a requirement for states to establish independent supervisory authorities, modelled closely on the lines of the 1995 Data Protection Directive, was introduced for the 1981 Convention in the 2001 Additional Protocol to that Convention, with the aim of bringing the Convention regime in this respect in line with the regime under the 1995 EC Directive (see Art. 1 AP) – although that of course only applies to those State-Parties to the original Convention that also acceded to the Protocol (as listed in footnote 46, above).

measures or regulations (Art. 28(2)) and had to be able to "***engage in legal proceedings***" in relation to alleged violations of their domestic data protection law (Art. 28(3), third bullet-point).

They were also put in charge of notification and "prior checking", as discussed under the next sub-heading.

Crucially also, apart from the more formal remedies noted under the next sub-heading after that, DPAs had to be given the right to "**hear claims [read: deal with complaints] lodged by any person**, or by an association representing that person" related to data protection (Art. 28(4)).

The DPAs, which at EU level worked together (until 25 May 2018) in the "**Article 29 Working Party**" discussed under the last sub-heading in the present section, have become the main defenders of data protection rights in the EU (even if their powers and effectiveness under the national laws adopted to implement the Directive still varied).

*NEW Notification and "prior checking"

*NEW *Notification:*

In order to achieve **general transparency** about the processing of personal data and to assist in ensuring full compliance with data protection law, the 1995 Data Protection Directive also provided for a broad system of **notification** of personal data processing operations (Art. 18, see Art. 19 for the details of the contents of notification); and stipulated that the notified particulars should be entered into a **register** that should be ***accessible to the public*** (Art. 21(2)). It was based on the system first adopted in Sweden in 1973, and taken up by many other EU Member States after that.

However, the Directive also allowed Member States, asalternatives to notification, to provide for ***simplifications*** or ***exemptions*** from the general notification obligation in (mainly) two "equivalent" situations, i.e.:[86]

- where, for "non-risky" processing,[87] the Member State's DPA had issued "***simplified norms***" setting out the basic parameters for the processing (i.e., the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored) (Art. 18(2), first bullet-point) – with controllers who formally declared that they abided by those simplified norms being **exempt** from notification; or
- where the Member State's law required the appointment of an independent ***data protection officer*** within the organisation of the controller, responsible for "ensuring in an independent manner the internal application of [the national data protection law adopted to implement the Directive] and for keeping a register of processing operations carried out by the controller, containing the same information as would otherwise have to be notified to the DPA (Art. 18(2), second bullet-point).

[86] The other operations that could be exempted from notification were **public registers**, processing of **records of members and associates of not-for-profit political, religious, philosophical or trade-union bodies (subject to some guaranties)**, and **manual files** (Art. 18(3) – (5)).

[87] Full text: "processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects".

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

The first exception was based on the French system of "*normessimplifiées*"; the second on the German system of requiring the appointment of Data Protection Officers within the organisations of all public- and most large private-sector controllers.[88] In relation to both alternative systems, the Directive stipulated that controllers (or some other body appointed by the Member State) should make the same information publicly available as would otherwise be accessible through the register of notified operations (Art. 21(3)).

*NEW *"Prior checking":*

In line with the French approach, the 1995 Directive required processing that posed "**specific risks to the rights and freedoms of data subjects**" ("**risky processing**") to be made subject to the further-reaching requirement of "**prior checking**" (Art. 20).It was left to the Member Statesto determine **which types of processing operations** they would submit to this further-reaching requirement (taking into account the purpose of the processing, the kinds of data, and the scale of the processing concerned). Member States could also choose**how and by whom** such a check would be carried out, in particular:

- whether to require a prior check ***upon submission of a notification*** indicating that the notified operation was of a kind that required such a check by the DPA (the French approach, followed by most other Member States); or
- if the processing was going to be regulated by a law or subsidiary legislative instrument, by the DPA in the course of the preparation of the instrument, or by Parliament, in the course of the adoption of such an instrument.

(Art. 20(2) and (3)).

Because of these various options in the Directive, the different Member States adopted (or rather, retained) different regimes in these regards, which meant that some operations were subject to notification or prior checks in some Member States, but not in others.

*NEW Specific remedies and sanctions

The 1981 Convention stipulated that the State-Parties to that convention should "*establish **appropriate sanctions and remedies***" for violations of their national data protection laws, but did not further clarify what would be "appropriate" in this respect.

By contrast to this stipulation in the 1981 Convention, the 1995 Directive stipulated that data subjects should have access to a **judicial remedy** for any (alleged) breach of their rights (quite apart from the right to lodge complaints with the relevant national data protection authority, noted under the previous sub-heading) (Art. 22). In addition, any person who suffered damage as a result of any unlawful processing or other act incompatible with the Directive should be entitled to obtain **compensation** from the controller (unless the latter could prove that he was not responsible) (Art. 23).[89] And beyond these remedies, the Member States were also required to provide for further "suitable measures" and

---

[88] Respectively referred to as *behördliche*- and *betrieblicheDatenschutzbeauftragten*, not to be confused with the state- and federal data protection authorities, *Landes*- and *Bundesdatenschutzbeauftragten*. Note that although many Member States introduced the concept of a DPO in the laws implementing the directive, they sis so in different ways, with different scopes and tasks for the DPO, and different conditions for their appointments. As discuss in Part Two, the GDPR in stead provides detailed, harmonised guidance on their appointment, and links this to the principle of "accountability".

[89] The UK initially tried to limit this to material damage only, but it was ultimately held that the Directive required that persons should also be able to obtain compensation from immaterial damage (distress).

"sanctions", irrespective of any individual claim or complaint (Art. 24).

However, in many Member States the actual penalties that could be imposed under the relevant national law, or that were imposed in practice, were relatively minor.[90]

*NEW The Article 29 Working Party and the Article 31 Committee

Finally, the 1995 Data Protection Directive established two EU-level entities, named after the articles under which they were created:

- the so-called "**Article 29 Working Party**", an independent groupcomposed of representatives of the Member States' data protection authoritiesas well as of the EDPS, and a representative of the European Commission (in charge of the group's secretariat, with no voting power), which was given the taskto contribute to more harmonised application of the Directive,in particular by adopting recommendations and opinions (on its own initiative) and give an opinion on any draft code of conduct elaborated at EU level; and which had to be consulted by the European Commission on any proposal in relation to "*the rights and freedoms of natural persons with regard to the processing of personal data*" (i.e., data protection) and on all draft decision on adequacy protection in a third country;[91] and
- the so-called "**Article 31 Committee**", composed of representatives of the Member States' governments, but chaired by a representative of the Commission, to which all draft measures to be taken under the Directive had to be submitted for an opinion; if the Committee issued a negative opinion, the measure had to be referred to the Council, where it could be overruled by a qualified majority.[92]

The **Article 29 Working Party** (WP29) has issued **numerous working documents and opinions** on an extremely wide range of issues relating to the application of the 1995 Data Protection Directive and the 2002 e-Privacy Directive (discussed at 1.3.3, below).[93] These documents, and especially the formal opinions, while not legally binding, are still highly authoritative in terms of the directives. They have helped to ensure that the directives are indeed fully and strictly applied, at a "high level", and they have to some extent mitigated the problems arising from the divergences in the laws of the Member States.

NB: The successor to the WP29, the European Data Protection Board (EDPB), builds on the work of the WP29: on its first day of existence, 25 May 2018, it endorsed a range of WP29 opinions that had been drafted in anticipation of the GDPR.[94] Its secretariat is provided by the EDPs.

---

[90] The need for stronger penalties only became apparent with the emergence of the Internet, largely controlled by non-EU/EEA entities that were less likely to comply with EU data protection rules merely at the urging of the EU DPAs. This is reflected in the much stronger stipulation in the GDPR that the DPAs can impose administrative fines of up to €10.000.000 or 2% of the annual turnover of the responsible actor, or indeed in especially egregious cases up to €20.000.000 or 4% of the annual turnover (Art. 83 GDPR).

[91] For details, see Article 30.

[92] For details, see Article 31.

[93] All Article 29 Working Party documents adopted between 1997 and November 2016 can be consulted on this archive page:
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm
Updates and documents adopted after November 2016, until the WP29 was abolished on 25 May 2018, can be found here:
http://ec.europa.eu/newsroom/article29/news-overview.cfm

[94] See footnote 248, below.

1.3.3 The 1997 Telecommunications Data Protection Directive, the 2002 EC e-Privacy Directive, and the 2009 amendments to the e-Privacy Directive

General

The **Telecommunications Data Protection Directive**, proposed at the same time as the 1995 Data Protection Directive, was adopted on 15 December 1997.[95] Its relationship to the 1995 Data Protection Directive was clarified in Art. 1(2), which said that the directive's provisions were to "*particularise and complement*" the main Directive. Specifically, the data protection-specific definitions in the 1995 Directive, and all other principles and rules in that directive, applied also to controllers and processing operations subject to the Telecommunications Data Protection Directive, except where the latter set out more specific rules. Also, in relation to specific purposes, features or services (itemised billing, calling line identification, directories, etc.: see below), the relevant provisions are all interpretations and applications of the general principles and rights in the 1995 Directive. In other words, the Telecommunications Data Protection Directive was a *lexspecialis* in relation to the 1995 Data Protection Directive, the *lexgeneralis*.

Implementation of this directive was delayed, partly because, in 1999, the Commission carried out a general review of the regulatory framework for electronic communications, in the light of developing new technologies and business practices. One result of this review was a proposal, in 2000, to replace the Telecommunications Data Protection Directive with a new directive concerning data protection in the electronic communications sector.[96] This led to the adoption, in July 2002, of the Directive on Privacy and Electronic Communications, Directive 2002/58/EC, generally referred to as the "**e-Privacy Directive**".[97] It, too, emphasised its subsidiary and complementary nature in relation to the main 1995 Data Protection Directive, in the same terms as its predecessor (see Art. 1(2)).

In 2009, the 2002 Directive was amended through a separate directive, Directive

---

[95] Full title: Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L24, 30.01.1998, pp. 1 – 8, available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0066&from=EN
The Telecommunications Data Protection Directive drew extensively on the work done within the Council of Europe on a recommendation on the same matter, which led to the adoption of Recommendation No. R (95) 4 of the Committee of Ministers of the Council of Europe to Member States on the Protection of Personal Data in the Area of Telecommunication Services, with particular reference to Telephone Services, adopted on 7 February 1995, available at:
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168050108e –
and on the work of DPAs in *the International Working Group on Data Protection in Telecommunications*(the "Berlin Group"), established in 1983, see:
https://www.dataprotectionauthority.be/berlin-group

[96] Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, Brussels, 12.07.2000, COM(2000) 385 final.

[97] Full title: 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 L201, 31.07.2002, pp. 37 – 47, available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN

2009/136/EC,[98] often referred to as the "**Cookie Law**" because it regulated cookies (although it also regulated further additional matters and data processing activities). In the text below we will describe the rules as they are contained in the 2002 Directive as amended by the 2009 Directive. For brevity's sake, we will from time to time refer to the 1995 Data Protection Directive as the "main directive", and to the e-Privacy Directive (as thus amended) as its "subsidiary" directive.

At the time of writing (December 2018), the e-Privacy Directive is still in force, even though its "mother" instrument, the 1995 main Data Protection Directive has been replaced by the General Data Protection Regulation. A successor to the e-Privacy Directive, to also be a regulation (rather than a directive) is in the process of being adopted (see section 1.4.2, below). However, because the e-Privacy Directive is still in force for the time being, it is still given full attention in this first edition of the handbook, and why, pending the adoption of the proposed new e-Privacy Regulation, we shall describe the still-applicable e-Privacy Directive in the present tense below.

Aim, purpose and scope of the 2002 e-Privacy Directive as amended in 2009

Whereas the main 1995 Data Protection Directive applied broadly, to all processing of personal data by any relevant public- or private-sector entity active in the "First Pillar" of the European Community, the e-Privacy Directive, as a subsidiary instrument, has a much narrower (more specifically-defined) scope. In its own words, it applies to:

> the processing of personal data in connection with the provision of **publicly available electronic communications services in public communications networks** in the Community, *including public communications networks supporting data collection and identification devices*.
>
> (Article 3, emphasis added; the words in italics were added by the 2009 amendment)[99]

The term "electronic communications service" is precisely, and strictly, defined in Article 2(c) of the revised Framework Directive,[100] as follows:

> 'electronic communications service' means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; **it does not include information society**

[98] Full title: 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 L337, 18.12.2009, pp. 11 – 36, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0136

[99] An exception for analogue exchanges, contained in the original (2002) version of the e-Privacy Directive, was removed by the 2009 amendments.

[100] Full title: Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.04.2002, pp. 33 – 50, available at: https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:32002L0021

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

> **services, as defined in Article 1 of Directive 98/34/EC,[101] which do not consist wholly or mainly in the conveyance of signals on electronic communications networks** (emphasis added)

The simple conclusion that follows from this stipulation in Article 3 and the definitions in these instruments was drawn by the WP29 in its 2011 Opinion on Geolocation services on smart mobile devices:[102] the e-Privacy Directive applies to providers of e-communication services such as telecommunications operators and Internet access providers, but not to providers of information society services.[103]

(As further discussed in section 1.4.2, below, the Commission proposes to remove this limitation under the proposed e-Privacy Regulation, but until that is done it remains in place.)

Within this limited scope, the e-Privacy Directive has the same aims as the main Directive: to ensure at the same time a ***high level of protection*** for personal data (but here specifically for that sector) and to enable the ***free flow of personal data*** within the Community (within that sector) (Cf. Art. 1(1)). It has had a major impact on the fast-growing, ever-more-important e-communications field, ensuring a higher level of data protection that field within the EU than anywhere else in the world.

That said, in spite of the seemingly clear language of Article 3, the question of the precise scope of the e-Privacy Directive is not completely clear, because some of its provisions apply – or are read as applying – more broadly; and because the e-Privacy Directive does not contain an explicit provision with regard to the applicable law. Without detracting from the success of the e-Privacy Directive, these ambiguities should be briefly noted.

Ambiguity and lack of coherence as to scope

First of all, there is ambiguity as to the material scope of the e-Privacy Directive.

As the Commission noted in its proposal for an e-Privacy Regulation:[104]

> Consumers and businesses increasingly rely on new internet-based services enabling inter-personal communications such as Voice over IP, instant messaging and web-based e-mail services, instead of traditional communications services. **These Over-the-Top communications services ("OTTs") are *in general* not subject to the current Union electronic communications framework, including the ePrivacy Directive.**

A 2013 study commissioned by the Commission (The SMART Study) found that:[105]

---

[101] Full title: Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, OJ L 204, 21.07.1998, pp. 37 – 48, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31998L0034

[102] Article 29 Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices (WP185, adopted on 16 May 2011), available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

[103] WP29 Opinion 13/2011 on Geolocation services on smart mobile devices (previous footnote), section 4.2.1, *Applicability of the revised e-privacy directive* (pp. 8 – 9).
As further discussed in section 1.4.2, below, the Commission proposes to remove this limitation under the proposed e-Privacy Regulation, but until that is done it of course remains in place.

[104] Proposal for an e-Privacy Regulation (footnote 154, below), section 1.1, p. 1, emphases added.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

> **national provisions on topics such as cookies, traffic and location data, or unsolicited communications, adopted pursuant the e-Privacy Directive, frequently have a different scope of application than the one defined by Article 3 of the e-Privacy Directive**, which is limited only to providers of publicly available electronic communication services (i.e. traditional telecoms companies). [The study found] that the limitation of the scope of the Directive only to providers of electronic communications services is ambiguous and may give rise to unequal treatment if information society service providers using the Internet to provide communication services are generally excluded from its scope.

There is also a lack of clarity as to the applicable national law.

Until the e-Privacy Directive is replaced by the proposed e-Privacy Regulation (which may not be for some time), the ambiguities and unclarities noted above will remain, and the effectiveness of the e-Privacy Directive will remain hampered by this.

Relationship between the e-Privacy Directive and the GDPR

The e-Privacy Directive was a *lexspecialis* in relation to the *lexgeneralis* of the 1995 Directive, and is therefore also a *lexspecialis* in relation to the latter's successor, the GDPR. Regarding matters specifically governed by the e-Privacy Directive, the e-Privacy Directive therefore appliesinstead of the GDPR provisions. Thus, the legal grounds of the GDPR are not applicable where the e-Privacy Directive provides more specific rules for the processing of personal data. For example, Article 6 e-Privacy Directive that sets forth a specific list of legal grounds regarding the processing of traffic data, including traffic data that constitutes personal data, applies and, consequently, Art 6 GDPR does not apply. However, in all other cases concerning the processing of personal data, the GDPR applies.

The same applies as concerns **entities that are, or are not, "*specifically governed by the e-Privacy Directive*"**. In view of the opinion of the WP29 that the e-Privacy Directive essentially only applies to providers of e-communication services, this means that similarly (other than in relation to the special rules in Article 5(3) and 13 which apply more broadly), processing of any data, including data more specifically regulated by the e-Privacy Directive (such as traffic data) by *entities other than e-communication service providers* is subject to the GDPR rather than the e-Privacy Directive, in spite of the special provisions in the e-Privacy Directive relating to such data.

In other words:

- e-communication service providers must abide by the e-Privacy Directive in relation to any matters that are more specifically regulated in that directive, and by the GDPR in relation to all other matters; and
- entities that are not e-communication service providers must abide by the stipulations in Article 5(3) of the e-Privacy Directive regarding access to information on devices and Article 13 of that directive as concerns unsolicited communications, and by the GDPR in relation to all other matters (i.e., they are not subject to any of the provisions in the e-Privacy Directive other than these two provisions).

---

105 "e-Privacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071) (hereafter referred to as the "SMART Study"), summarised at and available from: https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data (for the full report, follow the links at the bottom of the page)

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Specific issues in which the above questions arise are noted where relevant in the other subsections in this section.

Key features of the e-Privacy Directive[106]

Definitions

Since the e-Privacy Directive was expressly conceived as a *lexspecialis* to the *lexgeneralis* of the 1995 Data Protection Directive, the **data protection-relateddefinitions** from the 1995 Data Protection Directive also applied in relation to the e-Privacy Directive, as is expressly stipulated in Art.2, first sentence of the e-Privacy Directive. However, now that the 1995 Data Protection Directive has been replaced by the GDPR, all references to the definitions in that directive should be construed as references to the corresponding (but in certain respects updated and strengthened) definitions in the regulation. This is noted below under the separate heading of "*Consent*" in particular.[107]

Apart from this, the **definitions of the more technical e-communication-related terms** in the Framework Directive for Electronic Communications Networks and Services[108] that was the outcome of the review mentioned above, under the heading "*General*" – ***electronic communications service***;[109]***publicly available electronic communications service***; ***public communications network***; etc. – also apply to the relevant technical terms used in the e-Privacy Directive. This includes the term "**subscriber**" (to an e-communication service).

In addition, in Article 2, the e-Privacy Directive adds a number of *NEW**further (new) definitions**, such as "***user***", "***traffic data***", "***location data***", "***value-added service***", and "***personal data breach***" (see the article for details).

*AMENDEDConsent

The most important change to the definitions of core concepts in the GDPR compared to those in the 1995 Data Protection Directive concern the definition of "**consent**" as a legal basis for processing of personal data.

Specifically, Article 2(f) of the e-Privacy Directive provides that 'consent' by a user or subscriber as used in that directive corresponds to the data subject's consent in the Data Protection Directive. Because all references to the Data Protection Directive must now be construed as references to the GDPR, consent under the e-Privacy Directive must therefore now be understood in the same way as consent under the GDPR, where it is defined as:

> any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (Art. 4(11) GDPR)

---

106 Many of the requirements of the e-Privacy Directive noted here were already contained in the 1997 Telecommunications Data Protection Directive and merely carried over to the e-Privacy Directive, but this is not further noted each time. When an issue or provision is flagged up as "*NEW" this means that it is or introduces something that was not (yet) addressed in the 1995 Data Protection Directive.

107 The GDPR also somewhat further clarifies the concept of "personal data", by making clear that a person can also be "identifiable" by means of an "online identifier" (Art. 4(1) GDPR, Art. 2(a) of the 1995 Data Protection Directive). This too should now be taken into account also in the application of the e-Privacy Directive.

108 Footnote 100, above.

109 This term was discussed above, under the heading "*Aim, purpose and scope of the e-Privacy Directive*".

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

The GDPR also clarifies in more detail what conditions must be met before any consent can be deemed to be valid and specifies, among others, what it means for consent to be freely given, and what could constitute a clear affirmative action.[110]The European Data Protection Board (EDPB) has moreover issued guidelines on consent.[111]

These clarifications in the GDPR and in these guidelines are particularly relevant in relation to several key provisions of the e-Privacy Directive that require consent of the user or subscriber. These include:

- Article 5.3 for the storing or collecting of information from terminal equipment;
- Articles 6 and 9 for re-using traffic- and location data for value-added services of for the purpose of marketing electronic communications services;
- Article 12 for directories of subscribers; and
- Article 13 for unsolicited communications.

In relation to these matters, consent, in order to be valid, now needs to be "GDPR consent" – and the Member States are required to review the national laws transposing the e-Privacy Directive and national enforcement practices in order to ensure that they comply with the GDPR.

The above-mentioned matters are further discussed under the corresponding headings, below.

Security

Article 4(1) effectively repeats the data security requirement of the 1995 Data Protection Directive, by stipulating that providers of e-communications services must take "***appropriate technical and organisational measures to safeguard security of its services***", while adding that "*if necessary*", this must be done "*in conjunction with the provider of the [relevant] public communications network*". It also adds, just like the main Directive, that the level of security must be "***appropriate to the risk presented***", taking into account the state of the art and the cost of the measures. Article 4(1a), introduced by the 2009 Directive, adds that:

> Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least:
>
> - ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,
> - protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and,
> - ensure the implementation of a security policy with respect to the processing of personal data.

Both the e-Privacy Directive (in Article 4) and the GDPR (in Articles 32 – 34) provide for an

110 See Articles 7 and 8 GDPR, and related recitals 32 – 33, and 42 – 43.

111 EDPB Guidelines on Consent under Regulation 2016/679 (wp259rev.01). These Guidelines were adopted by the Article 29 Working Party (WP29) on 28 November 2017 and revised on 10 April 2018. They have been subsequently endorsed by its successor, the European Data Protection Board (EDPB). They complement a previous Art 29 WP opinion on the definition of consent (WP187, opinion, 15/2011).

obligation to ensure security, as well as an obligation to notify personal data breaches[112] to the competent national authority and the supervisory authority [i.e., the data protection authority], respectively.[113] These obligations will co-exist in parallel under the two different pieces of legislation, according to their respective scopes of application. Following Article 95 of the GDPR, the GDPR shall not impose additional obligations on natural or legal persons in relation to matters for which they are subject to specific obligations set out in the e-Privacy Directive. However, as a *lexspecialis* to the GDPR, the e-Privacy should [also] not lead to a lower level of protection than the protection the GDPR provides for.

Article 4(1) also stipulates that:

> Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.

Note that those "relevant authorities" need not be the national data protection authorities. See under the heading "*Supervision and enforcement*", below.

*NEW Risk notification

Article 4(2) of the e-Privacy Directive stipulates that:

> In case of **a particular risk of a breach of the security of the network**, the provider of a publicly available electronic communications service must **inform** the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of **any possible remedies**, including an indication of the likely **costs** involved. (emphases added)

This "risk notification" requirement (which was already included in the original 2002 text) should be distinguished from the more elaborate "data breach notification" requirements, discussed under the next heading – which were only added in the 2009 amendments, and which only apply once a breach has occurred, whereas Article 4(2) requires notification of any risk that a breach *may* occur.

*NEW Data breach notification

The e-Privacy Directive (as amended in 2009) stipulates that, in addition to the "risk notification" requirement discussed above, providers of e-communication services must ***notify the "competent national authority"*** of a – read *any actual* – personal data breach "*without undue delay*" (Art. 4(3), first sub-clause – note that this authority again need not be the DPA).

If (but only if) "*the personal data breach is **likely to adversely affect the personal data or privacy of a subscriber or individual***", then the provider must also "***notify the subscriber or individual***"of the breach "without undue delay" (Art. 4(3), second sub-clause). However, such notification to the subscriber or individual concerned is not required:

> if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such

112 The data breach notification requirements are discussed under that heading, later in this section.

113 On the different authorities involved in the enforcement of the e-Privacy Directive, see the next quote in the present sub-section and the comment on it, and the discussion under the last heading in this section.

> technological protection measures shall render the data unintelligible to any person who is not authorised to access it. (Art. 4(3), third subclause)

In other words, subscribers and other affected individuals (in particular of course, data subjects, but also legal entities that are subscribers) need not be informed of a data breach involving their data if the provider can prove to the "competent authority" that the data that have been compromised (in particular, any data that may have been improperly disclosed or made accessible to third parties) were **rendered completely "unintelligible"** to any person or persons who may have obtained access as a result of the breach, by appropriate technological protection measures (as clarified in Article 4 of Commission Regulation 611/2013).[114]

Conversely, the "competent authority" can "require" a provider to notify a data breach to the relevant subscribers and other affected individuals when the provider has not done so – i.e., because the authority does not agree with the assessment of the provider that the data breach was not "*likely to adversely affect*" the personal data or privacy of those subscribers or individuals, or because the authority does not believe that any leaked data are really completely "unintelligible" to the unauthorised recipient(s) (e.g., because the decryption key was or may have also been leaked, or because the encryption method was not sufficiently robust)[115] (Art. 4(3), fourth sub-clause).

The final, fifth sub clause of Article 4(3) stipulates that:

> The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

The e-Privacy Directive as amended by the 2009 Directive also provides for important **formal requirements** to back up the above new stipulations. Thus:

> [The competent national authorities] shall also be able to **audit** whether providers have complied with their notification obligations under this paragraph, and shall impose appropriate **sanctions** in the event of a failure to do so.

---

[114] Full title: Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, OJ L 173 of 26.06.2013, pp. 2 – 8, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0611
The Commission Regulation was adopted on the basis of Article 4(5) of the e-Privacy Directive, which empowered it to adopt "*technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements referred to in this Article*" (Art. 4(5)), after consulting the European Network and Information Security Agency (ENISA), the WP29 and the EDPS, and involving all (other) relevant stakeholders.

[115] For instance, weak algorithms such as MD5 or SHA1 are regarded as obsolete and data encrypted through them can no longer be regarded as having been made truly "unintelligible" (read: un-decryptable). See:
https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet
One can also think of a case in which e-communications data are breached, in which the content of the communications was fully encrypted by means of strong algorithms such as SHA-256, but the metadata were not. Note that (as pointed out on the above website) "the classification of a 'strong' cryptographic algorithm can change over time".

(Article 4(4), first sub-clause, second sentence, emphases added)

The effectiveness of these audit (inspection) and sanction powers is underpinned by a further requirement, set out in the second sub-clause of Article 4(4):

> Providers shall maintain an **inventory of personal data breaches** comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of paragraph 3. The inventory shall only include the information necessary for this purpose. (emphasis added)

The amended e-Privacy Directive provides for the issuing of "**guidance**" and "**instructions**" by the "competent national authorities" on "*the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made*" (Art. 4(4), first sub-clause, first sentence).

The above data breach notification requirements of the e-Privacy Directive, which are limited by the scope of that directive, foreshadow the more general data breach notification requirements now included in the General Data Protection Regulation, applicable to any personal data processing operation, discussed in Part Two, section 2.1, below. They can be considered to be redundant.[116]

Specific requirements for processing for specific purposes:

Rather than repeating the general data protection principles and the list of bases for legal processing that are set out in the main 1995 Data Protection Directive, the e-Privacy Directive lays down a general requirement of confidentiality of communications, and a series of specific requirements and conditions for certain specific data or processing operations. In these, the e-Privacy Directive seeks to apply the principles and rights of the 1995 Data Protection Directive to those specific matters, with the aim of harmonising the application of those principles and rights in the Member States, as discussed under the various headings, below.

First, however, it is important to recall that, to the extent that the e-Privacy Directive provides for specific legal grounds for processing for specific purposes (as set out in that directive), the more general legal grounds for processing for various purposes set out in Articles 5 and 6 of the GDPR do not apply.[117]

Thus, where the e-Privacy Directive requires consent – as in relation to access to information on devices (Art. 5(3)), or the sending of unsolicited marketing messages (Art. 13) – or sets out a range of specific legal bases and purposes of processing – as in relation to the processing of traffic data (Art. 6) – any entity subject to those rules – which in relation to Articles 5(3) and 13 is any entity, and in relation to Article 6 are providers of e-communication services – cannot rely on any other ground or principle, set out in the GDPR. In particular, they cannot rely on the "compatible purposes" ground for processing, set out in Article 5(1)(b) GDPR.

*NEW ***Confidentiality of communications:***

Article 5(1) of the e-Privacy Directive underlines the fundamental importance of

---

116 European Commission, REFIT analysis of coherence of the e-Privacy Directive with the GDPR (Chart – comment on Article 4.3.; 4.4.; 4.5 – Notification of personal data breaches).

117 See the sub-section on "*Relationship between the e-Privacy Directive and the GDPR*", above.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

confidentiality of communications – enshrined in many constitutions, at least in respect of the mail and telephone calls (though often now extended expressly or through interpretation to all forms of communication)[118] – by stipulating that Member States must:

> ensure the **confidentiality of communications and the related traffic data** by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, ***they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users***, without the **consent** of the users concerned, except when legally authorised … (emphases added)

As the words "*listening, tapping [etc.] … by persons other than users*" make clear, this provision does not just apply to providers of e-communication services. Rather (subject to the exceptions noted below), the Member States must, under their national laws, prohibit such interferences with the right to confidentiality of communications by **anyone**, including both state agencies and private entities such as companies.

Article 5(1) allows as an exception "*technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality*". There is a further exception in Article 5(2) in relation to recording of communications and traffic data to provide evidence of a commercial transaction or business communication. The so-called Data Retention Directive, briefly discussed at 1.3.4, below, provided for a further, sweeping mandatory exception to this prohibition of interception and collecting of communications data, but was declared void by the Court of Justice, as discussed in that section.

*NEW ***The use of "cookies" and other intrusive technologies:***

The amended e-Privacy Directive stipulates, in Article 5(3), in rather technical terminology, that Member States must ensure that:

> **the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user** is only allowed on condition that the subscriber or user concerned has given his or her **consent**, having been provided with **clear and comprehensive information**, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing.

The Directive clarifies in the next sentence in this paragraph that:

> This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

Note that the phrases "*for the sole purpose*" and "*as strictly necessary*" emphasise that this exception must be very narrowly applied.

The phrase "*the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user*" is technical language for technologies that allow a visitor to a website to be recognised by the website and tracked while using the website oreven across websites. The main means used to this are so-called

---

[118] Cf. the extensive interpretation of the concept of "correspondence" in Article 8 ECHR by the European Court of Human Rights in the famous case of *Klass v. the Federal Republic of Germany* (judgment of 6 September 1978), para. 41, where the Court held that "*telephone conversations … are covered by the notions of 'private life' and 'correspondence' [in that article]*".

"**cookies**" – which is why the 2009 Directive that strengthened the rules in this regard (as discussed below) was initially generally referred to as the EU's "**Cookie Law**", and is still sometimes referred to as such (so does, for instance, a private entity's website on the matter[119]).

In fact, there are a range of cookies that arise from technical international standardised tools called "RFC" adopted by the Internet Engineering Task Force (IETF) that may be considered in daily language to range from highly intrusive "**third-party tracking cookies**" to **non-intrusive ones** that improve the operation of websites without tracking the visitor[120]; and there are other intrusive technologies such as "**flash cookies**", **HTML5 storage methods**and so-called "**evercookies**"[121]. They all fall within the definition of "*information stored in the terminal equipment*", and therefore (somewhat problematically) are all treated the same under the e-Privacy Directive.[122]

The purpose and meaning of Article 5(3) is explained in simpler language in recitals (24) and (25) to the e-Privacy Directive, which make clear that it extends well beyond "cookies". They are worth quoting in full:

> Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called **spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.** (emphasis added)
>
> However, such devices, **for instance so-called 'cookies'**, can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar

---

119 See, e.g.: https://www.cookielaw.org/the-cookie-law/

120 See these IETF Recommendations on cookies (starting with RFC 2109 of 1997) which contain a non-exhaustive concept of privacy but also include some useful mandatory data in cookies:
https://tools.ietf.org/html/rfc2109 (the original RFC 2109);
https://tools.ietf.org/html/rfc2965 (RFC 2965, replacing RFC 2109 but keeping the same list of data); and
https://tools.ietf.org/html/rfc6265 (RFC 6265 of 2011, again keeping the original list, but with the introduction of third party accessing to the cookie – the currently in force recommendation).

See also this Wikipedia page:
https://en.wikipedia.org/wiki/HTTP_cookie
This gives extensive detail on all the various types of cookies**: session cookies**, **persistent cookies**, **secure cookies**, **HTTP-only cookies**, **Same-site cookies**, **Third-party cookies**, **Supercookies**and **Zombie cookies**; and provides detailed technical information.

121 See:
https://webcookies.org/doc/eu-web-cookies-directive

122 This may change under the proposed new e-Privacy Regulation, which could treat different technologies differently according to their relative intrusiveness.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

> device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information[, offering a right to refuse][123] or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose. (emphasis added)

The main change brought about by the 2002 Directive was that it changed the regime covering the use of such technologies from one where the subscriber or user had to be informed and given a "right to refuse" the setting of cookies (etc.),[124] to the one now in Article 5(3), under which cookies are only allowed provided that the subscriber or user was not only informed, but gave **positive, explicit consent**, in accordance with the conditions for (valid) consent set out in the main 1995 Data Protection Directive,[125] which defined consent as:

> any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed (Art. 2(h))

However, in view of the replacement of the 1995 Directive with the GDPR, the question arises whether this should now be read as requiring **the more demanding form of consent stipulated in the Regulation**. If that is the case, consent for the placing of cookies and such other tools should now be based on a:

> freely given, specific, informed and **unambiguous** indication of the [subscriber or user's] wishes by which he or she, **by a statement or by a clear affirmative action**, signifies agreement to the [placing of the cookie or the use of the other tools][126]

The above should mean that the use of "pre-ticked" boxes for the use of cookies etc. will no longer meet the consent requirements of the e-Privacy Directive.

However, there is still the issue in that the-Privacy Directive basically treats all "cookies" and tracking tools alike, without distinguishing between, say, "session cookies" and "persistent cookies". In practice,the provision has led to a "take it or leave it" culture on the Internet, in which website visitors are effectively forced to click "*I agree*" (to the placing of usually unspecified types of "cookies") in order to gain access to a site (including even sites of public

---

123 On the retention of the offering of a right to refuse, see the next two footnotes.

124 In the original 2002 version, the first sentence of Article 5(3) read:
*Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with and comprehensive **information** in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered **the right to refuse** such processing by the data controller.* (emphases added)

125 This change is not reflected in the recitals quoted in the text, which were not changed from the original 2002 Directive and still refer to the "right to refuse", even though this was removed by the 2009 Directive. In effect, those words have become dead letters.

126 Cf. Article 4(11) GDPR. Emphases added.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

bodies). The SMART Study found that:[127]

> the rules on cookies and similar techniques may have not entirely achieved their objectives, given that users receive too many warning messages which they do not properly consider.

Whether this will change under a new e-Privacy Regulation still remains to be seen – but of course these matters relate directly to the application of all the basic data protection principles and rights – including purpose-limitation, data minimisation, retention limitation, etc., e.g., in respect of issues such as what retention periods are appropriate for different cookies (depending on their purpose),[128] how valid consent ("GDPR consent") for the use of different cookies should be obtained, and how data subjects should be enabled to exercise their rights, etc. – and how these matters can and should be implemented on the basis of Data Protection by Design and Default – the principle now expressly enshrined in the GDPR.

*NEW ***Limitations on the use of traffic- and location data:***

Article 6 of the e-Privacy Directive imposes strict data limitation and -retention restrictions on the processing of traffic- and location data by providers of e-communication services. In principle, **traffic data** (i.e., data processed for the purpose of – and necessary for – the conveyance of a communication or for billing) may only be processed and stored by the provider of the relevant e-communications service for the purposes of the ***transmission*** of an e-communication, ***billing*** of the subscriber for the communication, or to enable ***interconnection payments*** (i.e., payments between providers for the use of each other's networks) (Art. 6(1) and (2)). This processing does not require the consent of the subscriber or user of the service because it is necessary for the provision of the service. When they are no longer needed for those services, they must be "erased or made anonymous" (Art. 6(1)).[129]

Traffic data may only be used for ***marketing of e-communications services*** or for the provision of ***value-added services***, but in these cases only with the **consent** of the subscriber of user. Again, this means that now that the GDPR is fully applicable, it must conform to the GDPR requirements for valid consent, i.e., it that the relevant consent must now take the form of a:

> freely given, specific, informed and unambiguous indication of the [subscriber or user's] wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to [the use of his or her traffic data for marketing by e-communication service providers or the provision of a specific value-added service].

The e-Privacy Directive also stipulates that the service provider must **inform** the subscriber to or user of its services of the types of traffic data which are processed and of the duration of such processing; for processing based on consent (i.e., for marketing and value-added services: see above), this informing must be done ***prior to the obtaining of such consent*** (Art. 6(4)).

Finally, the e-Privacy stipulates that processing of traffic data for an e-communications

---

127 See footnote 105, above.

128 Some websites stipulate retention periods of 25 years, which is manifestly excessive, whatever the purpose.

129 On the problems with the rendering anonymous of such data, see the discussion of the issue in the context of the GDPR, in Part Two, section 2.1, below.

services provider for various **subsidiary purposes** related to the provision of the services (***billing***, ***traffic management***, ***customer enquiries***, ***fraud detection***, ***marketing*** and the provision of ***value-added services***), by members of staff of the provider, or of any processor engaged by the provider, must be **restricted on a "need to have access" basis**: each of those should only have access to such traffic data as they need for their specific task (Art. 6(5)). However, "competent [outside] bodies", such as those settling billing- or interconnection payments disputes, must of course be granted access to traffic data when necessary (Art. 6(6)).

The e-Privacy Directive is even more strict as concerns the processing of "**location data other than traffic data**", i.e. data processed in an electronic communications network that indicates ***the geographic position of the terminal equipment of a user*** (such as, typically, a mobile phone) but which is ***not processed for the purposes of conveying an e-communication or billing for such a communication***. Such data may only be processed when they are rendered ***anonymous***,[130] or, to the extent that they may be used for the provision of a ***value-added service***, with the **consent** of the users of or subscribers to such a service (Art. 9(1), first sentence). The e-communications service provider must again **inform** the users and subscribers of the details of the processing, prior to obtaining such consent (*idem*, second sentence). Those users and subscribers should moreover both be able to withdraw such consent at any time (*idem*, third sentence), and/or to temporarily switch off such location tracking, "using a simple means and free of charge" (Art. 9(2)). And again, the processing of such data must be restricted to staff of the e-communications services provider, or of the provider of the relevant value-added service (or of a processor engaged by either of those) (Art. 9(3)).

*NEW *Itemised billing*

Subscribers must have the right to choose to receive **non-itemised bills** (Art. 8(1), and Member States should also provide **other privacy-enhancing solutions** in relation to itemised bills (Art. 8(2), e.g., itemised bills that only show the country- or regional codes for outgoing calls, or that omit or obscure the last three digits of the number called,in order to both explain the amount of the bill and protect the privacy of the user (who may not be the subscriber or a member of the family).

*NEW *Calling and connected line identification and automatic call forwarding*

e-Communication services providers must offer both callers and called individuals (including callers from within the EU [then EC] making calls to third countries) **the option to prevent calling line identification by the called person**, but people receiving a call from an unidentified number (originating from either within or without eh EU/EC) must be able to **block** the call; and people must be able to **switch off** their own calling line identification on a call-by-call basis (Art. 8(1) – (4)).

Providers of e-communications services must moreover **inform the public** (and of course in particular their subscribers and users) of these options (Art. 8(6)).[131]

---

130 See previous footnote.

131 These options were originally developed by national DPAs. Interesting enough those options, in contrast to the technical cookies standards, as soon as the services of "caller identification" etc. were commercially offered in the 1980s, they were integrated into the technical international standards for

Subject to relevant national rules (and, of course, to the general principles of necessity and proportionality), e-communication service providers may **override blocks** on calling line identification, either upon application of a subscriber, ***to trace malicious or nuisance calls*** (to allow for investigations of complaints by providers and the police, and to provide evidence for court cases), or to assist the ambulance services and fire brigades ***to respond to emergency calls*** (Art. 10(1) and (2)).

Subscriber must also have "*the possibility, using a simple means and free of charge, of **stopping automatic call forwarding** by a third party to the subscriber's terminal*" (Art. 11).

All the above mandatory options have been carried over into international technical norms so that can now be easily exercised in practice in relation to smartphones etc.

*NEW ***Directories of subscribers***

As a result of pressure from national DPAs, the e-Privacy Directive includes provisions under which subscribers must be informed of any intention to include their data (i.e., their landline or mobile phone number) in a **directory of subscribers** that is either ***publicly available*** or ***accessible through directory enquiry services***; and they must be able to not be included in such directories (i.e., **to "go ex-directory"**), free of charge and without having to provide reasons for this (Art. 12(1) and (2)).[132]

These rights apply to natural persons – but Member States must also make arrangements to ensure that "the legitimate interests of subscribers other than natural persons [i.e., of 'legal persons' such as companies]" are also "sufficiently protected" in these respects (Art. 12(4)).

If a directory is to be used for "***any purpose … other than the search of contact details** of persons on the basis of their name and, where necessary, a minimum of other identifiers*" – e.g., if those data are to be used for ***direct marketing***, ***credit scoring***[133] or ***political campaigning*** – the subscribers must be asked for **additionalconsent**, specifically for the use of their data for such other purposes (Art. 12(3)).[134]

*NEW ***Unsolicited communications***

---

transmission of telecom transmission (old-fashioned landlines), and then when mobiles appeared, into the mobile phones for activating the options. This was thanks to the regulators of France and of Germany which raised these issues with the telecom negotiators in Europe who then pushed those complete and easy-to-use solution at the global level, through GSM norms.

[132] The battle by DPAs for those protections took place before the 1997 Telecom Directive was adopted. In Germany, the focus was on not having to provide reasons to be excluded from telephone directories. In France, the main issue was the stipulation that this should be free of charge. During the negotiations on the Telecom Directive, France nearly succeeded to abandon the whole directive for that reason only. As a matter of fact, not being in a telephone directory led at that time to less number of communications – so less telecom profits at a time when telephone calls where paid one by one – while about 20% of subscribers where asking not to be in a telephone directory. With today's Internet, it is all the more important that users are not bothered with telephone calls if their telephone numbers are published.

[133] Cf. "**red-lining**": the practice of giving differential treatment in lending, housing, insurance and other services based on a person's address and that areas' default history – a practice made illegal in the USA many years ago. See, e.g.,:
https://www.investopedia.com/terms/r/redlining.asp
Also: *How Redlining's Racist Effects Lasted for Decades*, NY Times, 24 August 2017, available at:
https://www.nytimes.com/2017/08/24/upshot/how-redlinings-racist-effects-lasted-for-decades.html
(with maps illustrating the practice)

[134] A question remains whether this also applies to "legal persons", since this paragraph is not mentioned in the fourth paragraph of Article 12.

As noted at 1.3.2, above, the 1995 Data Protection Directive already gives data subjects an unconditional **right to object** to the use of any of their personal data for direct marketing purposes (Art. 14(b) of the 1995 Directive) – meaning marketing of any nature, commercial, political or otherwise At the time, this still mostly related to marketing by post. The e-Privacy Directive adds to this a requirement of **prior consent** for the use of ***automated calling machines*** and ***faxes***[135] or ***email*** ("electronic mail") for such purposes (Art. 13(1)). The reason is that sending messages by these means is much cheaper than using traditional mail, and therefore likely to increase their use. This requirement applies in relation to both natural and legal persons (individuals and companies, etc.). Moreover, as noted earlier, under the heading "*Aim, purpose and scope of the e-Privacy Directive*", this provision applies to **any entity** that wants to use any such means for the sending of direct marketing messages.

However, if a customer provides electronic contact details (phone number or email addresses, etc.) to a company in the context of a sale of a product or a service, the seller may use those details for **marketing of its own similar products or services** to such a customer (so-called "***proximity marketing***"), provided the customer is offered an easy means of objecting to such approaches in each communication (i.e., unless an "***opt-out***" from further marketing is offered in each communication) (Art. 13(2)).

With regard to other forms of direct marketing (i.e., non-"proximity" direct marketing and marketing using other means than automated calling- or fax machines or email), Member States can **choose** between a prior consent (i.e., an "***opt-in***" that is offered at the time of collecting the personal data) and an ("informed but did not object") "***opt-out***" model (Art. 13(3)).[136] However, the sending e-mail direct marketing messages "*disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease*", must always be prohibited (Art. 13(4)).

Derogations:

Article 15 of the e-Privacy Directive makes clear that Member States may restrict the various rights granted and obligations imposed by the directive on the same basis as under the broad "**important public interests**" derogation clause in the main 1995 Data Protection Directive (Art. 13), i.e., "*when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard* ***national security*** *(i.e. State security),* ***defence****,* ***public security****, and* ***the prevention, investigation, detection and prosecution of criminal*** **offences**" – to which the e-Privacy Directive merely adds: "*or* ***of unauthorised use of the electronic communication system***". The underlined words are reinforced in the e-Privacy Directive by the added express stipulation that:

> All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.(Art. 15(1), last sentence)

---

135 A "facsimile machine" or "fax" is a machine that allows an image (often an image of a document) to be sent over a telephone network. These days its use is rare. See: https://faxauthority.com/fax-history/

136 The EU "opt-out" model requires the informing of data subject of: (i) the intention to use their data for direct marketing; (ii) their right to opt out of such marketing; and (iii) details of how to (simply and free of charge) exercise this right. Note that the European "opt-out" model differs fundamentally from the U.S. one, which does not require the informing of data subjects of any of these details.

The articles in the TEU referred to refer to, respectively, the EU Charter of Fundamental Rights (announced in 2000, i.e., after the coming into force of the 1995 Data Protection Directive) and the European Convention on Human Rights.

While this is a welcome express acknowledgment of the crucial, EU-constitutional requirement to respect fundamental rights and freedoms, it is of course not really new: the relevant rule-of-law principles were in practice (and in law) already applied also at the time of the adoption of the "mother" Directive, as "general principles of Community law.[137]

Article 15(1) also stipulates that, in order to safeguard the various "important public interests" listed, but subject to the crucial *caveat* about respect for human rights and general principles of Community law:

> Member States may, *inter alia*, adopt legislative measures providing for **the retention of data for a limited period** justified on the grounds laid down in this paragraph.(Article 15(1), second sentence)

This original text, with its **explicit rule of law limitations,effectively prohibiting indiscriminate data retention**, is important in view of the subsequent attempts by the European legislator to impose precisely such indiscriminate data retention obligations under the so-called Data Retention Directive, ultimately declared void by the Court of Justice, as discussed at 1.3.4, below.

*DIFFERENCE***Supervision and enforcement***

Whereas the 1995 Data Protection Directive was enforced by specialist, independent data protection authorities and the GDPR is enforced by those same authorities, the EU Member States could choose to place supervision and enforcement of the e-Privacy Directive in the hands of a different body, or indeed of different bodies. This has led to different allocations of supervision to different authorities in relation to different issues covered by the e-Privacy Directive in the Member States.

The Commission found that "the allocation of enforcement competences to a wide range of authorities that often overlap", too, appeared to have "[hampered] the effectiveness of the rules in cross-border cases".[138]

Application of other main elements of the 1995 Data Protection Directive:

Finally, in this overview of the rules in the e-Privacy Directive, it should be noted that the e-Privacy Directive expressly stipulates that the requirements of the 1995 Directive with regard to **judicial remedies, liability and sanctions** (set out above, in section 1.3.2) shall also apply in relation to the e-Privacy Directive (Art. 15(2)); that the **Article 29 Working Party** (also discussed in that section) shall carry out its tasks as set out in the 1995 Directive also in relation to the e-Privacy Directive (Art. 15(3)); and that member States must provide for "effective, proportionate and dissuasive" penalties for infringement of the Directive (Art. 15a).

137 See footnote 66, above.
138 *Idem*.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

1.3.4 Third-Pillar data protection instruments[139]

In the period from the mid-1990s to 2009, the EU established a considerable number of bodies aimed at facilitating cooperation between the Member States in the area of police and criminal law ("Justice and Home Affairs" or JHA) – the so-called "Third Pillar" of the EU[140] – all centred on the establishment of pan-EU personal databases and rules and procedures for access to those databases by and exchanges of personal data between the Member States.

These included *Europol* (1998), the *Schengen Information System, SIS-I* (2001, updated to *SIS II* in 2013), *Eurojust* (2002), *Eurodac* (2003), the *Visa Information System, VIS* (2004) and the *Customs Information System, CIS* (2009).

In this period, the Council adopted some 123 instruments in the JHA area.[141] In 2005, the *Prüm Convention* was signed by seven Member States and by its Decision of 23 June 2008 the European Council agreed to integrate the main provisions of the Prüm Convention into the EU's legal framework, to enable wider exchanges (between all EU Member States) of biometric data (DNA and fingerprints) in the fight against terrorism and cross border crime.

In 2008, an overarching Framework Decision was adopted by the Council to establish common principles for the protection of personal data in the JHA area.[142] However, although many of the rules in the 2008 Framework Directive were inspired by Directive 95/46/EC and the Council of Europe Convention, as the then European Data Protection Supervisor, Peter Hustinx, observed, "*the level of protection was much lower in terms of scope and substance.*"[143] As to the scope, he pointed out that:[144]

> the Decision only applies when personal data are transmitted or made available to other Member States, and therefore does not extend to 'domestic' processing [i.e., processing by and within a Member State], unlike Directive 95/46/EC.

In 2009, following the entering into force of the Lisbon Treaty that ended the three-pillar structure,[145] a five-year transitional period commenced, during which JHA EU law was to be brought within the proper supranational EU legal-constitutional framework (see section 1.4.2, below).[146] In 2018, the 2008 Framework Decision was replaced by a new Decision (*idem*).

---

139 For details of the law in this area, see the historical sections in the relevant chapters in: Steve Peers, (2016). EU Justice and Home Affairs Law: Volume I: EU Immigration and Asylum Law (Fourth Edition) and Volume II: EU Criminal Law, Policing, and Civil Law (Fourth Edition), both Oxford University Press, 2016.

140 See footnote 58, above.

141 See Emilio De Capitani, Metamorphosis of the third pillar: The end of the transition period for EU criminal and policing law, *EU Law Analysis blogspot*, 10 July 2014, available at: https://eulawanalysis.blogspot.com/2014/07/metamorphosis-of-third-pillar-end-of.html

142 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*, OJ L 350, 30 December 2008, p. 60, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0977

143 Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, p. 15, available at: https://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf

144 *Idem*, with reference to Recital 7 and Article 1 of the Framework Decision.

145 See again footnote 58, above.

146 See Protocol 36 to the Lisbon Treaty and Emilio De Capitani, o.c. (footnote 141, above).

(CC) Douwe Korff & Marie Georges/Final Text as approved – 190723

1.3.5 Data protection in the Second Pillar

An informal system for "European Political Cooperation" (EPC) in external matters was in place from 1970 – 1993. Under the Maastricht Treaty that came into force in the latter year, this was formalised in the "Common Foreign and Security Policy" (CFSP) – the EU's "Second Pillar". However, until the further development of the CFSP under the 2009 Lisbon Treaty (which abolished the "pillar" structure),[147] as discussed in section 1.4.4, below, there were no specific data protection rules that applied to the processing of personal data in this area(other than the Member States' own data protection laws and the Council of Europe Convention).

1.3.6 Data protection for the EU institutions

There were no comprehensive or coherent data protection rules applicable to the EU institutions themselves until 2001, when a Regulation – Regulation (EC) 45/2001 – first introduced such rules, on the basis of Article 286 of the TEU, which required such rules.[148]

The data protection rules in the 2001 Regulation were based on the then-existing Community rules on data protection which applied to the Member States, in particular the 1995 Data Protection Directive and the 2002 e-Privacy Directive.

Regulation 45/2001 also established the European Data Protection Supervisor as an independent supervisory authority with the responsibility of monitoring the processing of personal data by the Community institutions and bodies, and required the designation of a Data Protection Officer (DPO) by each of those institutions or bodies.

Regulation (EC) 45/2001 was repealed by Regulation (EU) 2018/1725, which entered into force in 11 December 2018, as discussed in section 1.4.5, below.

1.4 Data protection law for the future

By the end of the first decade of the 21st Century, it became clear that the essentially 20th-Century data protection instruments, discussed in section 1.3, above, were no longer sufficient: they had been conceived and drafted before mass access to the Internet (or at least the world-wide web), ubiquitous (and mobile) computing, "Big Data", the "Internet of Things" (IoT), in-depth profiling, algorithmic decision-making and "Artificial Intelligence" (AI). Both in the EU and in the Council of Europe, new or updated ("modernised") data protection instruments were therefore prepared, as discussed in this section.

1.4.1 The EU General Data Protection Regulation

The European Commission proposed the adoption of a General Data Protection Regulation (GDPR) in 2012,[149] to meet the challenges posed by the new technologies and services. It

147 See again footnote 58, above.

148 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 *on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*, OJ L 8, 12 January2001, p. 1–22, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001R0045

149 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, 25.01.2012, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN
At the same time, the Commission also proposed a separate data protection instrument, a Proposal for a Directive on "the protection of individuals with regard to the processing of personal data by competent

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

saw strong, high-level data protection as an essential condition for gaining trust in the online environment, which itself is "*key to economic development*"; the new, updated *lexgeneralis* data protection regime was to play "*a central role in the Digital Agenda for Europe, and more generally in the Europe 2020 Strategy*".[150]

The background, status and approach and key elements of the GDPR are described in some detail in Part Two of this handbook. Suffice it to note here that the GDPR significantly **expands on and strengthens the main principles and rules**; expressly **adds genetic and biometric data to the list of sensitive data** (this was inspired by the work on the "modernised" Council of Europe Data Protection Convention, discussed below, at 1.4.3); aims to bring about **greater harmonisation** of data protection law in the EU Member States (at least in the areas where it applies, which is broadly the area previously referred to as the "First Pillar" of the European Communities), in line with the important new case-law of the Court of Justice – albeit subject to a wide range of ***"specification clauses"***(i.e., provisions leaving the more detailed regulation of certain matters to Member States' laws, within the overall frameworks of the GDPR, the EU treaties as interpreted by the CJEU and the Member States' own national constitutional and general legal systems;[151] provides for **stronger (and some new) data subject rights**; enables **much closer cross-border cooperation** between the Member States' data protection authorities (DPAs); and should result in **better, more consistent application and enforcement** of the rules.

More specifically, as already noted in the Introduction to this handbook, the GDPR introduces (or at least, makes much more specific) **the – now fundamental and mandatory in all member states – "accountability" principle**, and in many cases (including in relation to all public authorities subject to the Regulation) now ***requires*** the institution of **controller- or processor-appointed data protection officers** (**DPOs**).

As further explained in Part Two, the two are linked: under the GDPR, the DPOs will be the people who in practice will have to ensure compliance with the accountability principle by and within the organisations to which they belong.

1.4.2 The proposed EU e-Privacy Regulation

Although, as noted in the previous sub-section, one of the main aims of the proposed GDPR was to address the challenges posed by **the lack of trust (in particular, consumer trust) in the online environment**, it took the Commission another five years to propose a new instrument to replace the rules that are most specifically relevant to that environment, i.e., the e-Privacy Directive (Directive 2002/58/EC), discussed in section 1.3.4, above (which therefore remain in force in a somewhat "orphaned" way).

This came in the form of a proposal released in January 2017, to replace the e-Privacy Directive, too, with a regulation, the **proposed e-Privacy Regulation**.[152]

---

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, (COM(2012) 10 final) – but this directive is not discussed in this handbook (see the Note in the box on "*About this handbook*", on p. 1 of the handbook).

[150] Proposal for a GDPR (previous footnote), pp. 1 – 2 (with references to the main documents on the Digital Agenda and the Europe 2020 Strategy). The successor to the Digital Agenda is the Digital Single Market Strategy ("DSM Strategy").

[151] See Part Two, section 2.2, below, under the sub-heading "*… but with "specification clauses*".

[152] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

The proposal is still in the early phases of the legislative process: at the time of writing (December 2018), it was still being discussed internally within the Council) and subject to much attention from both proponents (civil liberties-, consumer- and digital rights groups)[153] and opponents (including some of the major U.S. "Internet Giants", who are asking either for a complete withdrawal of the proposal or its significant watering down).[154] It is therefore really too early to discuss the proposed regulation here in detail: undoubtedly, the final version will in at least some respects probably be quite different from the proposal.

It will therefore have to suffice, for this first edition of the handbook, to simply present the **key points of the Commission proposal**, as set out by the Commission itself:[155]

> The proposal for a regulation on high level of privacy rules for all electronic communications includes:
>
> - **New players:** privacy [*and data protection*] rules will in the future also apply to new [*so-called "Over-The-Top" or OTT*] players providing electronic communications services such as WhatsApp, Facebook Messenger and Skype. This will ensure that these popular services guarantee the same level of confidentiality of communications as traditional telecom operators.
> - **Stronger rules:** all people and businesses in the EU will enjoy the same high level of protection of their electronic communications through this directly applicable regulation. Businesses will also benefit from one single set of rules across the EU.[156]
> - **Communications content and metadata:** privacy is guaranteed for communications content and metadata, e.g. time of a call and location. Metadata have a high privacy component and is to be anonymised or deleted if users did not give their consent, unless the data is needed for billing.[157]
> - **New business opportunities:** once consent is given for communications

---

2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, Brussels, 10.01.2017, available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN

153 See the Open letter to European member states on the ePrivacy reform, sent by a large group of non-governmental organisations on 27 March 2018, available at:
https://edri.org/files/eprivacy/20180327-ePrivacy-openletter-final.pdf

154 See: Corporate Europe Observatory, *Shutting down ePrivacy: lobby bandwagon targets Council*, 4 June 2018, available at:
https://corporateeurope.org/power-lobbies/2018/06/shutting-down-eprivacy-lobby-bandwagon-targets-council

155 https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation (bold original; words in square brackets and italics and footnotes added)

156 But note that this will depend on the rules in the e-Privacy Regulation not containing "flexible"/"specification" clauses such as are contained in the GDPR (see Part Two, section 2.1, below). If the final text of the e-Privacy Regulation were to contain such "flexible" provisions (as is very likely), it would be crucial – especially for the online environment, which is by its very nature transnational – to add an "applicable law" provision.

157 But note the continuing attempts by the Member States and the Commission to retain or re-introduce mandatory e-communications (meta-)data retention: see section 1.3.4, above.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

data - content and/or metadata - to be processed, traditional telecoms operators will have more opportunities to provide additional services and to develop their businesses. For example, they could produce heat maps indicating the presence of individuals; these could help public authorities and transport companies when developing new infrastructure projects.

- **Simpler rules on cookies:** the cookie provision, which has resulted in an overload of consent requests for internet users, will be streamlined. The new rule will be more user-friendly as browser settings will provide for an easy way to accept or refuse tracking cookies and other identifiers. The proposal also clarifies that no consent is needed for non-privacy intrusive cookies improving internet experience (e.g. to remember shopping cart history) or cookies used by a website to count the number of visitors.
- **Protection against spam:** this proposal bans unsolicited electronic communications by emails, SMS and automated calling machines. *Depending on national law* people will either be protected by default or be able to use a do-not-call list to not receive marketing phone calls.[158] Marketing callers will need to display their phone number or use a special pre-fix that indicates a marketing call.
- **More effective enforcement:** the enforcement of the confidentiality rules in the Regulation will be the responsibility of data protection authorities, already in charge of the rules under the General Data Protection Regulation.

1.4.3 The Law Enforcement Data Protection Directive of 2016 (LEDPD)

Introduction

Article 10(1) of Protocol 36 to the 2009 Lisbon Treaty provided for a transitional period before the full powers of the Commission and of the Court of Justice applied to the EU legal acts in the field of police cooperation and judicial cooperation in criminal matters adopted before the entry into force of the Lisbon Treaty (the "former third pillar *acquis*"). This transitional phase came to an end on 1 December 2014.

In 2012, the Commission submitted its proposals for a directive in this area together with its proposal for a General Data Protection Regulation (introduced in section 1.4.1,above, and discussed in more detail in Part Two of this handbook).[159] However, like the GDPR, the Law Enforcement Data Protection Directive, LEDPD (also referred to as the "Law Enforcement Directive", LED, the "Data Protection Police Directive", or even just as the "Police Directive") was only adopted in 2016, onthe same day as the GDPR.[160] Unlike the GDPR which, as a

[158] This is precisely such a "specification clause" as mentioned in section 1.3.3, above, under the heading "*Complications*" – and illustrates the need for an "applicable law" rule to clarify which of the different national rules will apply to cross-border marketing mailings.

[159] See footnote 149, above.

[160] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, OJ L 119, 4 May 2016, p. 89–131, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

regulation, is in principle directly applicable in the legal orders of the Member States (albeit, in that case, with a significant number of clauses that actually still need further "specification" in national law),[161] the LEDPD, as a directive, does not apply directly (i.e., it has no "direct effect") but rather, **must be "transposed" into national law**. This had to be done within two years of the formal entering into force of the directive, i.e., by 6 May 2018 (just a few weeks before the GDPR came into application, on 25 May of that year).

Note however the extensive longer implementation periods provided for in Articles 61 – 63 of the Directive, due to different circumstances surrounding the huge number of data processing operations involved, which will be briefly discussed at the end of this section on the LEDPD, under the heading "*Delayed transposition*".

Here, it must suffice to note the main characteristics and requirements of the LEDPD.[162]

A Directive instead of a Council Framework Decision

The first point to be made is that setting out the rules for processing of personal data in a directive is in itself a **significant improvement** on having them contained within a Council Framework Decision such as the 2008 one revoked by the LEDPD.[163] As a directive, it can be invoked in national courts (and ultimately in the Court of Justice) by individuals in actions against the State; and it is subject to the enforcement powers of the Commission, which are aimed at ensuring that such instruments are properly transposed into national law.

Scope of the LEDPD

i. Activities covered

In relation to scope, the LEDPD stipulates the following:

Scope

1. This Directive applies to the processing of personal data by competent authorities [for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security].
2. This Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
3. This Directive does not apply to the processing of personal data:
   (a) in the course of an activity which falls outside the scope of Union law;

The Directive formally entered into force the day after its publication in the Official Journal, i.e., on 5 May 2016 – but as noted in the text, it only had to be applied in practice (through transposition into the domestic law of the Member States) two years after that date, i.e., by 6 May 2018.

[161] See Part Two, section 2.2., below.

[162] As explained at the beginning of this handbook, we hope to expand on EU data protection law outside of the GDPR in a second edition. That would expand in particular on the rules in the LEDPD that are only briefly summarised here.

[163] See Steve Peers, *The Directive on data protection and law enforcement: A Missed Opportunity?*, Statewatch Analysis blog, April 2012, available at: https://www.statewatch.org/analyses/no-176-leas-data%20protection.pdf

(b) by the Union institutions, bodies, offices and agencies.[164]

Within a "competent authority" the precise demarcations between data processing subject to the LEDPD and those subject to the GRPD has tobe assessed taking into account Recital (12). This makes clear, in its last sentence, that processing of personal data in relation to "*other tasks*" entrusted to the "competent authorities", which are "*not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security*", is subject to the GDPR rather than the LEDPD.

Controller will have to give close attention to this delineation, and to other questions such as the extent to which collecting and further processing of personal data in relation to "incidents" in relation to which it is *not yet clear* whether any offences occurred, or in relation to the taking of measures (including "*coercive measures*") at demonstrations or major sporting events that "*may lead to a criminal offence*" (*or not*), are subject to the LEDPD – because the answers to those questions have a major impact on the level of data protection that must be ensured, e.g., in terms of informing data subjects, data retention limitations, restrictions on data subject rights, etc.. In the meantime, Data Protection Officers working within the relevant authorities should seek to assist the authorities in making these determinations, with a view to ensuring appropriate levels of data protection in all contexts.

The concept of "**public security**" is usually used in the context of exceptions to EU law, i.e., to indicate grounds that can be used to justify an activity that otherwise would be in breach of Union law. As Koutrakis points out, "*[P]ublic security constitutes a ground for exceptions from all four freedoms under the Union's primary rules.*"[165] To quote a Briefing Paper, produced at the request of the IMCO Committee of the European Parliament:[166]

> Of all the grounds for exceptions from free movement, **public security is most closely associated with what is traditionally understood as the core of national sovereignty, that is, the sphere of activity within which the State has primary responsibility to protect its territory and citizens**. (emphasis added)

The leading **CJEU judgment** on the question of "public security" is the *Campus Oil Case*,[167] in which the Court held that a national measure – *in casu*, a national quota of refined oil provisioning in the Republic of Ireland – was justified because refined oil was considered:

---

[164] Processing by EU bodies, office and agencies for the purposes of the prevention, detection, investigation, and prosecution of criminal offences are subject to a special set of rules, contained in Chapter IX of the new regulation on the processing of personal data by EU institutions (etc.), Regulation (EU) 2018/1725, as briefly discussed in section 1.4.5, below.

[165] PanosKoutrakis, *Public Security Exceptions and EU Free Movement Law*, in: Koutrakos, P., Nic Shuibhne, N. and Sypris, P. (Eds.), Exceptions from EU Free Movement Law, 2016 (pp. 190-217), p.2, available at:
http://openaccess.city.ac.uk/16192/
(With reference to Arts. 36 (Goods), 45(3) and 52 (Persons), 62 (Services), and 65 TFEU (Capital)).

[166] Public Security Exception in the Area of non-personal Data in the European Union, Briefing Paper requested by the IMCO Committee of the European Parliament and prepared by Kristina Irion, PE 618.986, April 2018, p. 3, available at:
https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/618986/IPOL_BRI(2018)618986_EN.pdf

[167] Judgment of the Court of 10 July 1984, *Campus Oil Limited and others v Minister for Industry and Energy and others*, Case 72/83, ECR 1984 -02727, available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:61983CJ0072&from=EN

> **of fundamental importance for a country's existence** since not only its services but above all its institutions, its essential public services and even the survival of its inhabitants depend upon them. (para. 34, emphasis added)

This makes clear that, **on the one hand, the term "public security" as used in EU law is not limited to matters related to criminal activity, but extends to matters such as the protection of "essential public services" and measures aimed at ensuring "the survival of [a country's] inhabitants"; but on the other hand, it is not as wide as "public order" – a term often used in police law to refer to matters such as maintaining order at demonstrations, parades and festivities.**[168]**Rather, as the Council puts it, the issue to be protected must relate to:**[169]

> **a genuine and sufficiently serious threat affecting one of the fundamental interests of society, such as a threat to the functioning of institutions and essential public services and the survival of the population, as well as by the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations, or a risk to military interests.**

The assessment of the precise limits of what is and what is not covered by (criminal?) threats to "public security" raises difficult questions of assessment in specific circumstances. When does some public disorder – e.g., an interruption of flights by people demonstrating against the forced expulsion of asylum seekers – amount to a "threat to an essential publicservice?[170] And when is a risk of a "disturbance to foreign relations" – say, a demonstration against a state visit by a foreign head of state – sufficiently "serious" to be classified as a risk to public security?Yet the answers to these questions determine whether the LEDPD applies to any processing of personal data in relation to such actions, or not.

While many entities – in particular public-sector ones such as local authorities or environmental-, social welfare- or animal welfare bodies – are given some public authority and some public powers in relation to (certain) crimes and (certain) threats to public security, the main tasks of those authorities will not be related to the investigation (etc.) of criminal offences within their relevant remits, or to threats to public order (whether involving crime or not).

Data Protection Officers in such public authorities or -bodies should carefully examine to what extent the processing of personal data by their own organisation or organisations can be said to be subject to the GDPR, and to what extent it is subject to the LEDPD. This will often not be a straightforward issue to clarify, and the DPO should therefore work on this together with the controller, the relevant legal service and the competent supervisory authority. Moreover, personal data processed in processing operations that are subject to the LEDPD will generally have to be kept separate from personal data processed in

---

168 Cf., e.g.: http://www.lokalepolitie.be/5371/contact/diensten/20-handhaving-openbare-orde (in Dutch)

169 Council of the European Union, Interinstitutional File: 2017/0228 (COD), Recital (12a), at p.3 , available at: http://www.consilium.europa.eu/media/32307/st15724-re01en17.pdf

170 In the UK, there was controversy over the prosecution and conviction of precisely such demonstrators under anti-terrorism legislation – i.e., under "public security" law – rather than under the normal criminal law of trespass, see: https://www.theguardian.com/global/2019/feb/06/stansted-15-rights-campaigners-urge-judge-to-show-leniency
The case is the subject of an appeal.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

operations that are subject to the GDPR, with specific rules and policies on when the personal data in one category/for one purpose can be used in another category/for another purpose.[171]

Finally, an issue arises in relation to the boundary between the activities of the EU Member States in the area of "*prevention, investigation, detection or prosecution of criminal offences*" and "*safeguarding against and the prevention of threats to public security*", on the one hand, and Member States' activities concerning **national security**, and the activities of Member States' agencies or units dealing with national security issues, on the other. The lines between these two areas of activity – the first nominally fully within, the second formally totally without EU law – is increasingly blurred (especially in relation to not-very-sharply-delineated categories of "terrorism", "cybercrime", "cyber security", etc.).[172] In fact:[173]

> [I]n some countries, the agencies themselves are becoming hybrids, with the dual roles of fighting crime and protecting national security. The US Federal Bureau of Investigation (FBI) is a prime example[174] but in the UK, too, GCHQ is working increasingly closely with the law enforcement agencies.[175]

This issue cannot be discussed in detail here, but it will be touched upon in section 1.4.6, below, on transmissions of personal data by a controller in an area covered by one category of EU data protection law, to a controller subject by another category of EU law – or, in the case of national security agencies, not subject to EU law at all.

On the other hand, the distinction between processing of personal data covered by the

---

171 Cf. also the discussion in sub-section 1.4.6, below, on exchanges of personal data between different entities working in the different EU data protection regimes.

172 Douwe Korff, Ben Wagner, Julia Powles, Renata Avila and Ulf Buermeyer, Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes, comparative report covering Colombia, DR Congo, Egypt, France, Germany, India, Kenya, Myanmar, Pakistan, Russia, South Africa, Turkey, UK, USA, prepared for the World Wide Web Foundation, January 2017, in particular section 2.3.1, available at: https://ssrn.com/abstract=2894490

173 *Idem*, p. 27. The expanding of the role of the police into "preventive" action is not new. See Ian Brown & Douwe Korff, Privacy & Law Enforcement, FIPR study for the UK Information Commissioner, 2005, Paper No. 4, The legal framework, section 3.1. The more recent developments, in particular also in relation to the blurring of the lines between policing and activities relating to national security, are noted in Douwe Korff, Protecting the right to privacy in the fight against terrorism, Issue Paper written for the Commissioner for Human Rights of the Council of Europe, 2008, available at: https://wcd.coe.int/ViewDoc.jsp?Ref=CommDH/IssuePaper(2008)3

174 A page on the FBI website on "*Addressing threats to the nation's cybersecurity*" expressly notes that the FBI is charged both with protecting the USA's national security and with being the nation's principal law enforcement agency, adding that "*[t]hese roles are complementary, as threats to the nation's cybersecurity can emanate from nation-states, terrorist organizations, and transnational criminal enterprises; with the lines between sometimes blurred.*" See: www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity
The FBI has recently changed an FBI Fact Sheet to describe its "*primary function*" as no longer "*law enforcement*", but now "*national security*". See The Cable, 5 January 2014, at: http://thecable.foreignpolicy.com/posts/2014/01/05/fbi_drops_law_enforcement_as_primary_mission#sthash.4DrWhlRV.dpbs For the dangers inherent in such blurring of the lines, see: www.foreignpolicy.com/articles/2013/11/21/the_obscure_fbi_team_that_does_the_nsa_dirty_work [original note]

175 See Computer Weekly, "*GCHQ and NCA join forces to police dark web*", 9 Nov 2015, at: http://www.computerweekly.com/news/4500257028/GCHQ-and-NCA-join-forces-to-police-dark-web [original note]

LEDPD and processing of personal data by the EU institutions, bodies, offices and agencies is clear, with the latter covered by a new regulation adopted in 2018, as discussed in section 1.4.6, below.

ii. Entities covered

Also in relation to the issue of scope, the LEDPD defines the "**competent authorities**" referred to in Article 1(1) as:

> (a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or
>
> (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.
>
> (Article 3(7))

As already noted, this may extend far beyond the police and other first-line law enforcement agencies, to include, depending on thenational constitutional approach, local and regional public bodies, welfare-, health and safety agencies, bodies supervising financial institutions, animal welfare or the environment, customs and tax agencies, and many more – whenever they are granted "*public authority and public powers*" in relation to criminal offences or threats to public security that may involve criminal activity taking place within their remit.

As also already noted, processing of personal data by such bodies in relation to activities not relating to criminal matters is subject to the GDPR and not to the LEDPD, and the same may be the case with regard to processing of personal data by such authorities in relation to threats to public security that do not involve criminal offences – such as storms or floods or epidemics, or the handling of sporting events other than in relation to possible criminal acts.

iii. Processing operations covered

With regard to the means used for processing, in line with the other EU data protectioninstruments, the LEDPD applies to:

> processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

In other words, the LEDPD applies to **all processing of personal data by automated means** and to the processing of all personal data held in **structured manual files** that are within its scope in terms of activities and entities covered.

Importantly, unlike the 2008 Framework Decision discussed earlier, in section 1.3.6, above,**the LEDPD applies** not only to personal data that are exchanged between Member States, but **also to domestic processing of personal data for law enforcement purposes**. As the Commission points out, the Directive should consequently "*make cooperation easier for*

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

the police and criminal justice authorities across the EU".[176]

Free movement of data between competent authorities in different Member States

Although the Directive "*shall not preclude Member States from providing higher safeguards than those established in this Directive*" (Art. 1(3)), any Member State that does set such higher standards may not invoke them to "**restrict or prohibit**" the free exchange of personal data between Member States that is the very purpose of the Directive (Art. 1(2)(b)). On the other hand, if a Member State, in its law, provides for "specific **conditions**" for certain processing (e.g., for profiling) – or, presumably, for the processing of certain kinds of data (e.g., biometric data) – then that Member State not only may, but indeed must ("shall") also:

> provide for the transmitting competent authority to inform the recipient of such personal data of those conditions and [of] the requirement to comply with them.
>
> (Art. 9(3))

However, Member States may not, under this provision, impose conditions on recipients in another Member State that are involved in judicial or police matters, other than those it imposes on "similar transmissions" to domestic recipients of that kind (Art. 9(4)).

(On the question of transfers of personal data to non-EU countries, see under that heading, below.)

Content

Many provisions in the LEDPD are very similar to provisions in the GDPR – but only up to a point, to reflect the special context of law enforcement and the prevention of criminal threats to public security.

The **definitions** of the core concepts in Article 3 – "*personal data*", "*processing*", "*restriction of processing*", "*profiling*, "*pseudonymisation*", "*filing system*", "*controller*, "*processor*", "*recipient*", "*personal data breach*", "*genetic data*", "*biometric data*", "*data concerning health*" – are effectively identical to the definitions of those same concepts in the GDPR.[177]

The **basic principles**, set out in Article 4, are also similar. Notably, the principle of **"lawfulness"** – which was missing from the 2008 Framework Decision – is now expressly included in Article 4(a) and elaborated on in Article 8(1) – with the principle of "transparency" (which is directly associated with the principle of lawfulness and fairness in the GDPR)to some extent reflected in Article 8(2) ("*Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing*") and in the provisions on the informing of data subjects, and on the granting of access to their data (albeit that in the special context of the LEDPD these rights are subject to broader restrictions).

The **purpose-limitation principle islimited** in that personal data collected by any of the above-mentioned competent authorities for law enforcement or public security purposes

---

[176] European Commission, Factsheet - How will the data protection reform help fight international crime?, 30 April 2018, available at: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (Follow link)

[177] Oddly, while setting out all the above-mentioned definitions in essentially identical terms as in the GDPR, the LEDPD does not define "third party" – even though another definition (of "recipient") expressly mentions third parties.

may be used for any other purpose, as long as that is "*authorised by* [read: any] *Union or Member State law*" (Art. 9(1), first sentence), subject to the stipulation inArt.9(1), second sentence, that:

> Where personal data are processed for such other purposes, Regulation (EU) 2016/679 [the GDPR] shall apply unless the processing is carried out in an activity which falls outside the scope of Union law.[178]

It follows that any law enforcement data made available under such an "authorising" law must still be limited to what is "relevant" and "necessary" for the "legitimate" purpose pursued by the authorising law.**In principle, there is an important role here for the DPOs acting for, respectively, the disclosing and receiving entities.** However, in some countries the law may simply stipulate that certain law enforcement data must, in certain specified circumstance (e.g., when authorised by a senior official) be made available to non-law-enforcement agencies.[179]

The Directive requires Member States to set **data retention limits** for the data processed under the Directive (Art. 5); and to make **clear distinctions** between personal data of different **categories of data subjects**, such as suspects, persons convicted of a criminal offence, victims, witnesses, etc. (Art. 6); and it stipulates that "*Member States shall provide for personal data based on facts to be distinguished, as far as possible, from personal data based on personal assessments*" (Art. 7(1)).

The LEDPD also (like the GDPR) requires controllers to adopt **"state of the art" security**, taking into account the context and purposes etc. of the processing (Art. 29(1)), and must indeed carry out a **risk assessment** in that regard, in order to determine what level of security is appropriate (Art. 29(2)). It also (again like the GDPR) requires physical and technical security (*idem*) and the imposition of **confidentiality duties** on staff (Art. 23).

Also similar to the GDPR, **personal data breaches** must be reported to the supervisory authority within 72 hours (or if not done within that period, the delay must be justified) (Art. 30); and data subjects must be informed of them "*without delay*", "*where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons*" (Art. 31).

The rules in the LEDPD on the processing of **sensitive data** – i.e., of "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership," genetic data, biometric data (when used for the purpose of uniquely identifying a natural person), "data concerning health" and "data concerning a natural person's sex life or sexual orientation" – are framed somewhat differently from those in the GDPR (art 9),[180]in that the LEDPD allows the processing of such data:

---

178 See also Article 9(2). This is again further discussed in sub-section 1.4.6, below.

179 Cf. the discussion of (then proposed) wide data sharing on minors in the UK between social welfare-, educational- and police authorities in Ross Anderson *et al.*, Children's Databases – Safety and Privacy: A Report for the Information Commissioner, prepared by the UK Foundation for Information Policy research (FIPR), 2006, which includes summaries by Douwe Korff of not only the relevant data protection-legal rules in the UK (*Data Protection Rules and Principles Relating to Data Sharing*, p. 100ff.), but also (in an Appendix) an overview of *Regulation Elsewhere in Europe*, specifically in Germany and France, available at: https://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf

180 The LEDPD understandably does not contain a provision on the lines of Article 10, first sentence, GDPR, stipulating that the processing of personal data relating to criminal convictions and offences must be

> **only** where **strictly necessary**, subject to **appropriate safeguards** for the rights and freedoms of the data subject, and only:
>
> (a) where **authorised** by Union or Member State **law**;
>
> (b) to protect the **vital interests** of the data subject or of another natural person; or
>
> (c) where such processing relates to data which are **manifestly made public by the data subject**.
>
> (Art. 10 LEDPD, emphases added)

The latter two conditions correspond to exceptions in the GDPR (respectively, Art. 9(2)(c) and (e)).[181]

Where a Member State relies on the other condition – **authorisation by law** – it must be able to demonstrate that the data processing is "***strictly necessary***" and that any limitation related to any data subject's rights are "***subject to appropriate safeguards***". Moreover (different from the situation under the 2008 Council Framework Decision), individuals can now rely on the Directive to assert their rights, with the Court of Justice of the EU ultimatelybeing able to determine whether any national law adopted in this context meets the "*strict necessity*" standard and incorporates "*appropriate safeguards*"; and with the Commission being empowered to take enforcement action if it feels a Member State's law authorising processing of sensitive data for law enforcement/public security purposes does not meet those standards.

The LEDPD also, like the GDPR, regulates**automated decision-making including profiling**, but with some differences. Specifically, it stipulates that the such processing must be "*authorised by Union or Member State law*" and subject to "*appropriate safeguards*" which must include "*at least the right to obtain human intervention on the part of the controller*". However, unlike the GDPR, the LEDPD does not stipulates that, when there is such "human intervention", the data subject should be able to "*express his or her point of view and … contest the [automated/profile-based] decision*".

Notably, the LEDPD states that:

> **Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited**, in accordance with Union law. (emphases added)

In relation to the question of "authorisation by law", it is also important to take into account that the relevant Member State's**Data Protection Authoritymust be consulted** during the elaboration of legislative proposal on those matters (art.28.2).

DPOs in relevant authoritieshave to give careful consideration to the questionof how these important newrequirements of the LEDPD – human intervention and the duty of non-discrimination – can be really and effectively applied in practice in different contexts.

"*under the control of official authority or … authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects*": the LEDPD and the relevant national laws themselves ensure this. Similarly, there is no need to repeat in the LEDPD the stipulation in the last sentence of Article 10 GDPR, that "*Any comprehensive register of criminal convictions shall be kept only under the control of official authority*."

[181] Except that the exception relating to processing to protect the vital interests of the data subject or another person under Article 9(2)(c) GDPR only applies if "*the data subject is physically or legally incapable of giving consent*" – which is not required under the LEDPD.

Given its field of application, the LEDPD allows for quite extensive**limitations onthedata subject's rights** to be informed of processing, to be given access to his or her data, and to rectification or erasure of data that do not meet the relevant data quality standards, or are otherwise processed contrary to the rules set out in the instrument – but those limitations must still be limited to what is "necessary" and "proportionate" in a democratic society (see Articles 12 – 16 LEDPD and Article 15 in particular). The LEDPD also allows for the exercise of those rights to be exercised **indirectly**, through the relevant supervisory authority (Art. 17). Where the personal data are "*contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings*", the rights may also be regulated by relevant national law (Art. 18). Typically, **Police Laws** or **Criminal Procedure Codes** regulate access by a suspect, accused, charged, indicted or convicted person to certain parts of the relevant files, in certain phases of the proceedings (typically, allowing limited access in the early phases and broad access later, especially once a person is formally indicted) – and such arrangements can therefore be retained.

Practical and formal requirements

In many other respects, too, the LEDPD introduces practical and formal requirements similar to the GDPR.

In particular, very importantly, the LEDPD, like the GDPR, includes the new "**accountability principle**" (Art. 4(4))[182] and requires that, "*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons*", all controllers subject to the Directive must:

> … implement appropriate technical and organisational measures **to ensure and to be able to demonstrate** that processing is performed in accordance with this Directive.
>
> (Article 19(1), emphases added)

The article adds that "*[t]hose measures shall be reviewed and updated where necessary*"; and that "*where appropriate*", they must include the (drawing up, adoption and) implementation of "*appropriate data protection policies*" by the controller (Art. 19(1), last sentence, and (2)).

Also, like the GDPR, the LEDPD requires extensive **record- and log-keeping** (Arts. 24 and 25), which are important means to ensure verifiability of the legality of processing – which is particularly challenging in the area of application of the LEDPD.

The LEDPD lays downthe same requirements as the GDPRin relation to "**joint controllers**" (Article 21(1)) and the use of processors (Article 22).

The LEDPD requires the carrying out of a **Data Protection Impact Assessment (DPIA, A**rticle 27**)** in similar circumstances as envisaged in the GDPR, i.e.:

> Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is **likely to result in a high risk to the rights and freedoms of natural persons** (Art. 27, emphasis added)

The relevant **supervisory authority** (which may be the general national data protection authority, but could also be a separate one, provided conditions of independence etc. are met: see below) **must also be consulted**, when a DPIA "*indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk*"

[182] Discussed in detail in Part Two, section 2.3, below.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

or where (irrespective of such measures) "*the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects"* (Article 28(1)(a) and (b)).

As a means of contributing to itseffective application, in particular in relation tothe accountability principle, theLEDPD provides for the appointment of a **Data Protection Officer (DPO)** by each controller (Art. 32), clarifies the position of the DPO (Art. 33) and lists the tasks of the DPO (Art. 34). This too is in line with the GDPR, which requires the appointment of a DPO by all public-sector entities subject to it.[183]However, the LEDPD does not explicitly stipulate that the DPO must be able to act in an independent manner.[184]

DPOs in law enforcement agencies and any other agency or body subject to the LEDPD will have a major role to play in relation to compliance by their organisations with the accountability principle and the relevant on-going reviews of measures taken to comply with this principle;the drafting of the "arrangements" with any joint controller and of the contracts with processors; consultation with the DPA; and the carrying out of DPIAs under the LEDPD.[185]

International data transfers to competent authorities in third countries

Because of the high sensitivity of the context and of personal data at stake in this field, chapter V of the LEDPDprovides for a range of conditions for the transfer of personal data to a non-EU country ("third country") or international organisation, similar to the conditions for transfers in the GDPR, but with additional rules on the transfer to a third country or an international organisation by an EU Member State of personal data received from another Member State, and on onward transfers from and by the recipient third country to another third country or an international organisation – and with more specific exceptions for specific reasons, as discussed below.

Note however that in particular in respect of international data transfers, the LEDPD allows for prolonged delays to the full application of the rules discussed below, for specific reasons,as discussed under the heading "*Delayed transposition*" at the end of this section on the LEDPD.

General pre-conditions for any such transfer:

Article 35 LEDPD sets out**threepre-conditions** for transfers to a third country (but note that *two of those can be set aside in some circumstances*, as indicated):

- the transfer must be "**necessary**" for the purposes set out in Article 1(1), i.e., for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or to safeguard against or prevent (criminal-legal) threats to public security;
- the transfer must be to **an authority in the third country or international organisation competent for the above-mentioned purposes** (whereby the International Criminal Police Organisation, Interpol, is expressly included in this in

183 See Part Two, section 2.4.2, below.

184 Cf. Article 38(3) GDPR which stipulates that:
"*The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor*."

185 Cf. the detailed discussion of the tasks of the DPO under the GDPR in Part Three of this handbook.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Recital (25)).[186] Just as "competent authorities" in the EU are not limited to first-line law enforcement agencies, the authorities in third countries to which data may be transferred also need not be first-line law enforcement agencies, as long as they are competent (also) in relation to relevant criminal matters.

Note that *this pre-condition can be waived in certain situations*, under certain conditions, as discussed below under the sub-heading "*Transfers to other authorities*".

- "*where personal data are transmitted or made available from another Member State, that Member State has given its **prior authorisation** to the transfer in accordance with its national law*" (subject to an exception, as noted below).

  (Article 35(1)(a) – (c))

  This last stipulation relates to the transfer from one Member State to a third country or international organisation of personal data originally received from another Member State, i.e., the onward transfer of such data requires the "prior authorisation" of the Member State that originally provided the data.

  Note that *this prior authorisation is not required if*:

  > the transfer of the personal data is **necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State** and the prior authorisation cannot be obtained in good time.

  In such a case, "*[t]he authority responsible for giving prior authorisation [read: the authority that should have been asked for its prior agreement if there had not been such an immediate threat] shall be **informed** without delay*" (Art. 35(2), emphasis added).

Once these relevant pre-conditions are met, personal data may still only be passed on to a

---

[186] In this regard, it may be noted that **Interpol** is not an "international organisation" as normally defined in public international law, i.e., an organisation based on a treaty or otherwise established under international law: see Article 2 of the International Law Commission's Draft Articles on the Responsibilities of International Organisations. By contrast, Interpol was established by police authorities of the participating states. On this issue, see the question put to the Commission by Charles Tannock, MEP, on 15 October 2013, available at: https://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2013-011707&language=EN – and the answer give by the Commission, available at: https://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2013-011707&language=EN
But Interpol is still often treated as an international organisation, also to some extent by the EU, which has adopted a Council Common Position on the exchange of passport data with Interpol and Interpol member states, subject to data protection guarantees: Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol, OJ L 27, 29 January 2005, p. 61, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32005E0069 (on data protection, see Art. 3)
See also Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205, 7 August 2007, p. 63, which prohibits the transfer or making available of SIS-II data to third countries and international organisations (Art. 54), but makes an exception as concerns exchanges of data on stolen, misappropriated, lost or invalidated passports with Interpol (Art. 55), available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32007D0533
Recital (25) LEDPD suggests that under that instrument more personal data can be shared with – and through – Interpol, as long as the general conditions for data transfers to international organisations (and third countries) set out in the Directive (as discussed in the text above) are met.

third country or international organisation if **one of the followingthreeconditions**apply:

- the Commission has issued an **adequacy decision** in relation to the recipient third country or international organisation (as further regulated in Article 36).

  But note that *the European Commission has not yet made any such adequacy decisions under the Directive* so this clause cannot yet be relied on.

  Or:

- "**appropriate safeguards**" are in place to ensure that the personal data, after transfer, will still be processed subject to "appropriate" data protection safeguards.

  This is further clarified in Article 37 which stipulates that the relevant safeguards must either be set out in a **legally binding instrument** (which can be a treaty or a binding legal administrative agreement) (Art. 37(1)(a)) or "*the controller [must have] **assessed** all the circumstances surrounding the transfer of personal data and [has concluded] that appropriate safeguards exist with regard to the protection of personal data*" (Art. 37(1)(b)) – but in the latter case, **the supervisory authority** must be informed of the "categories of transfers" made under this clause. Furthermore, every such transfer must be "*documented and the documentation shall be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred*" – Art. 37(3)).

  Note that the "**legally binding instruments**" mentioned include "*international agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 6 May 2016*" as referred to in Article 61 LEDPD. Those agreements, that article says, "*shall remain in force until amended, replaced or revoked*" as long as they "*comply with Union law as applicable prior to that date*". The LEDPD does not set a date by when these agreements, if not in accordance with the rules in the LEDPD, should be amended, replaced or revoked – or even that the Member States must review them to that end. This is further discussed below, under the heading "*Delayed implementation*".

  Note also that the alternative "**appropriate safeguards**" relate only to data protection: there is no requirement (such as is imposed under the first two of the derogations discussed next) that an assessment is made of the possible impact on the data subject's other "fundamental rights and freedoms", and if so, whether perhaps those should "override the public interest in the transfer";

  Or:

- (in the absence of an adequacy decision pursuant to Article 36 and of appropriate safeguards in accordance with Article 37) if a **derogation for a specific situation** applies. Article 38 allows for such derogations if a transfer is "**necessary**" in **five situations**, two of which require a "balancing" of interests.In a different order from the one in the article, the special situations and conditions are as follows:

  - Personal data may be transferred to a third country without an adequacy decision and without appropriate safeguards if this is "**necessary**" for any of the purposes set out in Article 1(1), i.e., for the purposes of **the prevention, investigation, detection or prosecution of any criminal offences or the execution of any criminal penalties, or to safeguard against or prevent any (criminal-legal) threats to public security** (Art. 38(1)(d)) – unless:

    the transferring competent authority determines that fundamental rights

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

> and freedoms of the data subject concerned override the public interest in the transfer (Art. 38(2)).

- Personal data may be transferred to a third country without an adequacy decision and without appropriate safeguards if this is "**necessary**" for **the establishment, exercise or defence of legal claims** relating to any of the above-mentioned purposes (Art. 38(1)(e)) – again unless:

> the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer (Art. 38(2))

Note that the above two situations relate to cases posing serious human rights dilemmas: on the one hand, the transfer is "necessary" for a major public interest, but on the other hand, it affects the fundamental rights and freedoms of the data subject – perhaps in possibly terrible ways, as when information on a suspect, witness or victim is passed on to authorities in a state that seriously violates human rights; and there are no "appropriate safeguards" in place, even as concerns the (further) processing of the data subject's personal data. **Clearly,the DPO of the relevant authority should be consulted on such transfers, and will carry a heavy advisory burden in this regard.**

- Personal data may be transferred to a third country without an adequacy decision and without appropriate safeguards if this is "**necessary**" **for the prevention of an immediate and serious threat to public security of a Member State or a third country** (Art. 38(1)(c)) – *in this case apparently irrespective of any consideration of the fundamental rights and freedoms of the data subject (unless that can be read into the requirement of "necessity"?)*.

- Personal data may be transferred to a third country without an adequacy decision and without appropriate safeguards if this is "**necessary**" **in order to protect the vital interests of the data subject or another person** (art. 38(1)(a)).

- Personal data may be transferred to a third country without an adequacy decision and without appropriate safeguards if this is "**necessary**" **to safeguard legitimate interests of the data subject**, *where the law of the Member State transferring the personal data so provides* (Art. 38(1)(b)).

The data transferredon the basis of any of the above five derogations must be***"strictly necessary"*** (Recital (72)), and **documented**, and:

> the documentation shall be **made available to the supervisory authority on request**, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred. (Art. 38(3), emphasis added)

The purpose of this documentation and its availability to the supervisory authority is to allow the supervisory authority to (retrospectively) "*monitor the lawfulness of the transfer*" (Recital (72). Recital (72) adds that:

> [The derogations listed above] should be **interpreted restrictively** and **should not allow frequent, massive and structural t**ransfers of personal data, or large-scale transfers of data, but should be limited to data strictly necessary.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Again, any DPO in any relevant organisation would carry major responsibilities in respect of this documentation, and in any interactions on relevant issues with the supervisory authority.[187]

Transfers to other authorities in third countries

As noted earlier, in principle all the above kinds of transfers can only be made to authorities in the relevant third country that are granted competences in relation to the purposes listed in Article 1(1) of the Directive, i.e., in relation to "*the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of [criminal-legal?] threats to public security*" (Art. 35(1)(b)) (although the recipients do not need to be law enforcement agencies proper; they can include other public authorities with some tasks and powers relating to crime or public security).

However, Article 39 LEDPD allows for **exceptions** to this rule, under the heading "*Transfers of personal data to recipients established in third countries*" (meant are recipients other than authorities which, in the relevant third country, are competent for the matters listed in Article 1(1) of the Directive).

Recital (73) explains the reasons for these exceptions (paragraph breaks and emphasis added):

> Competent authorities of Member States apply bilateral or multilateral international agreements in force, concluded with third countries in the field of judicial cooperation in criminal matters and police cooperation, for the exchange of relevant information to allow them to perform their legally assigned tasks. In principle, this takes place through, or at least with, the cooperation of the authorities competent in the third countries concerned for the purposes of this Directive, sometimes even in the absence of a bilateral or multilateral international agreement.
>
> **However, in specific individual cases, the regular procedures requiring contacting such an authority in the third country may be ineffective or inappropriate, in particular because the transfer could not be carried out in a timely manner, or because that authority [read: the relevant law enforcement agency] in the third country does not respect the rule of law or international human rights norms and standards, so that competent authorities of Member States could decide to transfer personal data directly to recipients [read: other, non-law-enforcement entities] established in those third countries.**
>
> This may be the case where there is an urgent need to transfer personal data to save the life of a person who is in danger of becoming a victim of a criminal offence or in the interest of preventing an imminent perpetration of a crime, including terrorism.
>
> Even if such a transfer between competent authorities and recipients established in third countries should take place only in specific individual cases, this Directive should provide for conditions to regulate such cases.
>
> Those provisions should not be considered to be derogations from any existing bilateral or multilateral international agreements in the field of judicial cooperation in criminal matters and police cooperation. Those rules should apply in addition to the other rules of this Directive, in particular those on the lawfulness of processing and Chapter V.

[187] See Part Three of this handbook, *Tasks of the DPO*, Tasks 1 – 5 and 12.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Article 39(1) can be paraphrased as follows:[188]

> Union or Member State law may provide for law enforcement agencies, in individual and specific cases, to transfer personal data directly to recipients established in third countries that are not competent in relation to criminal- and public security matters, but only if the other provisions of this Directive are complied with and all of the following conditions are fulfilled: …

The LEDPD is silent on the precise nature of the relevant "other authorities".Given that Article 39 applies to situations that are particularly human rights-sensitive (see the sentence emphasised in bold in the quote from Recital (73), above), it is assumed that what is envisaged are recipients in the third country in which the transmitting authority in the relevant EU Member State has **special trust**. In particular, the transferring authority must feel confident that the recipient non-law-enforcement agency will not pass the information on to a law enforcement agency in the third country that "*does not respect the rule of law or international human rights norms and standards*".The relevant case-by-case assessment will always be an especially delicate one, that should at the very least be **most carefully documented** (including the reasons for assuming the data can be passed on to the trusted agency without fear of it ending up in the hands of less savoury bodies in the third country concerned).

For transfers not covered by international agreements (as discussed separately, below), Article 39(1) sets out **fivecumulativeconditions** for the relevant transfers. The data may be transferred to a relevant non-law-enforcement recipient in a third country if (emphases, clarifications in square brackets and notes under the clauses added):

a. the transfer is **strictly necessary** for the performance of a task of the transferring competent authority [in the relevant EU Member State] as provided for by Union or Member State law for the purposes set out in Article 1(1) [i.e., **in relation to EU- or Member State criminal matters or public security matters**].

b. the transferring competent authority determines that **no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand**.

   Note that this determination is not limited to the data protection interests of the data subject, but rather, should look more generally at whether the relevant third country, and specific agencies in that country "*respect the rule of law or international human rights norms and standards*". The determination should moreover be made on **a case-by-case basis**.

c. the transferring competent authority considers that the **transfer to an authority that is competent for the purposes referred to in Article 1(1)** [criminal- and public security matters] in the third country is **ineffective or inappropriate**, in particular because*the transfer cannot be achieved in good time* –

   or, one should add, because this would be "inappropriate" for other reasons: see the note under the next clause.

---

[188] The text of Article 39(1) reads as follows:
"*By way of derogation from point (b) of Article 35(1) and without prejudice to any international agreement referred to in paragraph 2 of this Article, Union or Member State law may provide for the competent authorities referred to in point (7)(a) of Article 3, in individual and specific cases, to transfer personal data directly to recipients established in third countries [other than law enforcement agencies] only if the other provisions of this Directive are complied with and all of the following conditions are fulfilled: …*"

d. **the authority that is competent for the purposes referred to in Article 1(1) in the third country is *informed*** without undue delay, unless this is **ineffective or inappropriate**.

   Note that the reference to transmission to a (law enforcement) agency that would normally be the most relevant and appropriate one being "**inappropriate**" may be read as referring to a situation in which that agency "*[does not] respect the rule of law or international human rights norms and standards*". The reference to "**ineffectiveness**" of that agency may refer to it being *otherwise ineffectual, slow, incompetent or perhaps corrupt*.

e. **the transferring competent authority informs the recipient of the specified purpose or purposes for which the personal data are only to be processed by the latter*provided that such processing is necessary***.

   Note that this implies that the receiving authority in the third country must provide (strong and binding) **assurances** that it will abide by these stipulations, and will really only use the data provided by the EU law enforcement body for the specific, stipulated purpose or purpose and for no other; and even then will only use the data to the extent that that is (strictly) necessary for the stipulated purpose of purposes.

In addition to meeting these specific stipulations, as noted, Article 39(1) stresses that "*[all] the other provisions of this Directive*" must also be complied with (see also the last sentence in Recital (73), quoted above, which stresses that this includes "in particular those [provisions] on the lawfulness of processing and Chapter V", i.e., the other provisions on data transfers).

All of the above is, however, "**without prejudice to any international agreement**" (Art. 39(1)), by which is meant:

> any bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial cooperation in criminal matters and police cooperation. (Art. 39(2))

This should be read together with Article 61, which deals with the LEDPD's "*Relationship with previously concluded international agreements in the field of judicial cooperation in criminal matters and police cooperation*" and which stipulates that:

> International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 6 May 2016 and which comply with Union law as applicable prior to that date shall remain in force until amended, replaced or revoked.

The LEDPD does not stipulate a date by when these agreements, if not in accordance with the rules in the LEDPD, should be amended, replaced or revoked – or even that the Member States must review them to in order to bring them into line with the Directive.[189] However, Article 62 LEDPD does stipulate that:

> By **6 May 2022**, and every four years thereafter, **the Commission** shall submit **a report on the evaluation and review of this Directive** to the European Parliament and to the Council. The reports shall be made public. (emphasis added)

[189] We are also not aware of any reviews done before the LEDPD was introduced, of whether the International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States before then complied with Union law as then applicable.

These reviews are to include "*in particular, the application and functioning of Chapter V on the transfer of personal data to third countries or international organisations*" (Art. 62(2)), with "particular regard" to adequacy decisions under Article 36(3) and to **transfers to "other authorities" under Article 39**, as just discussed. The Commission may, moreover, in that context, "*request information from Member States and supervisory authorities*" (Art. 62(3)) including, presumably, on the above-mentioned international agreements they have concluded. Also presumably, the Commission may, on the basis of the first review, **propose** that **changes** be made to those agreements, or at least make **suggestions** as to how they should be brought into line with the rules in the LEDPD – but this is not stipulated in the Directive (unlike in relation to Union acts in this area).[190]

According to the Commission, the LEDPD will lead to "**stronger international cooperation**":[191]

> Cooperation between EU police and criminal justice authorities with non-EU countries will also be strengthened [by the LEDPD] since there will be clearer rules for international data transfers related to criminal offences. The new rules will ensure that transfers take place with an adequate level of data protection.

However, as noted below under the heading "*Delayed transposition*", it will still take some time before the new rules referred to will actually fully apply.

Supervision and enforcement

Chapter VI of the LEDPD requires the establishment of **independent supervisory authorities** in the Member States charged with monitoring and enforcing the application of the provisions of the national laws adopted to implement ("transpose") the Directive, and other related tasks (See Arts. 41 – 46 LEDPD). The relevant supervisory authority or authorities may be, but need not be, the general supervisory authority or authorities established under the GDPR (Art. 41(3)): in some countries, there are special supervisory authorities to supervise police and law enforcement agencies' processing of personal data, while in others the general data protection authority (DPA) is also given this task. Moreover, in some countries (especially federal ones), there are different national (federal) and local or regional authorities.

Like the general DPAs appointed under the GDPR, the supervisory authorities competent in relation to the matters covered by the LEDPD must be given **extensive powers**, including a right to demand (and obtain) "***access to all personal data*** *that are being processed and to* ***all information*** *necessary for the performance of its tasks*"; and the power to issue ***warnings*** to a controller or processor, to ***order*** the controller or processor to ***change*** operations to bring them into line with the Directive, "*where appropriate, in a specified manner and within a specified period, in particular by ordering the rectification or erasure of personal data or restriction of processing*", and to impose ***a temporary or definitive limitation,***

---

[190] Article 62(6) stipulates that, by **6 May 2019**, the Commission must have reviewed such "*other legal acts adopted by the Union which regulate processing by the competent authorities for the purposes set out in Article 1(1) including those referred to in Article 60, in order to assess the need to align them with this Directive and to make, where appropriate, the necessary proposals to amend those acts to ensure a consistent approach to the protection of personal data within the scope of this Directive.*" See further under the heading "*Delayed transposition*".

[191] European Commission, Factsheet - How will the data protection reform help fight international crime? (footnote 176, above).

including a ban, on processing; and the power to ***initiate legal proceedings*** against controllers or processors who allegedly act in breach of the Directive, or to bring such matters to the attention of the relevant (prosecuting) authorities (Art. 47(1), (2) and (5) LEDPD). The supervisory authorities also have important **advisory functions** and must be given the right:

> to issue, on [their] own initiative or on request, **opinions to [their] national parliament and … government** or, in accordance with its national law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data. (Art. 47(3), emphasis added)

They must also publish an **annual report** on their activities, "*which may include a list of types of infringement notified and types of penalties imposed*" (Art. 49).

The decisions of the supervisory authorities must, however, be subject to "*appropriate safeguards, including effective judicial remedy and due process, as set out in Union and Member State law in accordance with the Charter*" (Art. 47(4)).

Notably, the LEDPD stipulates that:

> Member States shall provide for competent authorities to put in place effective mechanisms to encourage confidential reporting of infringements of this Directive. (Art. 48)

This stipulation is in line with the recently adopted Whistleblowing Directive.[192]

Article 50 provides for **mutual assistance** between the supervisory authorities of the EU Member States, competent in relation to processing of personal data that is subject to the LEDPD.

Moreover, the **European Data Protection Board**, established under the GDPR, is also given competence in relation to processing within the scope of the LEDPD (Art. 51). This includes the issuing of ***guidelines, recommendations and best practices*** on any matter raised under the Directive, and the issuing of:

> An **opinion for the assessment of the adequacy of the level of protection in a third country, a territory or one or more specified sectors within a third country, or an international organisation**, including for the assessment whether such a third country, territory, specified sector, or international organisation no longer ensures an adequate level of protection (Art. 51(1)(g)).

The Board must forward its opinions, guidelines, recommendations and best practices to the Commission (and to the Committee established under Article 93 GDPR), and must make them public (Art. 51(3)); and the Commission must in turn inform the Board of the action it has taken in response (Art. 51(4)).

Remedies, liability and penalties

Chapter VIII sets out the remedies, liabilities and penalties that must be provided in the national laws transposing the LEDPD.

---

192 Directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law, 2019. At the time of preparing this handbook, the text had not yet been published in the Official Journal (and therefore also does not yet have a number), but the text as adopted by the European Parliament on 16 April 2019 (which is the final text, subject to language editing and translation) is available at: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0366_EN.html?redirect

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Briefly, in line with the GDPR, every data subject must be granted **the right to lodge a complaint** with the relevant supervisory authority, if the data subject considers that the processing of personal data relating to him or her infringes provisions adopted pursuant to this Directive (Art. 52), as well as the right to obtain an **effective judicial remedy** against any legally binding decision of a supervisory authority concerning him or her (Art. 53), and against any controller or processor subject to (the national law transposing) the LEDPD, "*where he or she considers that his or her rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of his or her personal data in non-compliance with those provisions*" (Art. 54). Moreover (again in line with the GDPR):

> the data subject to have **the right to mandate a not-for-profit body, organisation or association** which has been properly constituted in accordance with Member State law, has statutory objectives which are in the public interest and is active in the field of protection of data subject's rights and freedoms with regard to the protection of their personal data **to lodge the complaint on his or her behalf and to exercise the rights referred to in Articles 52, 53 and 54 on his or her behalf**. (Art. 55, emphasis added)

Data subjects also have a **right to compensation** for material and non-material damages caused by processing contrary to the LEDPD (Art. 56).

Finally, Member States must provide for **"effective, proportionate and dissuasive" penalties** for any infringements of the LEDPD (Art. 57)

Delayed transposition

As already mentioned in earlier sub-sections, not all processing of personal data for law enforcement and public security purposes does yet have to be in accordance with the LEDPD or the national laws transposing the LEDPD: the Directive contains a range of provisions allowing for certain instruments and operations to only be brought into line with the Directive at some future date (or indeed in some undefined future). The provisions allowing for delayed implementation relate to EU "legal acts"; treaties between EU Member States and third countries or international organisations (including Interpol); and special Member States' automated processing systems in the criminal law and public security area.

Delayed implementation in relation to EU legal acts:

Article 60 LEDPD stipulates in relation to the approximately 123 EU instruments ("legal acts" of varying types) relating to Justice and Home Affairs (JHA) matters[193] that:

> The specific provisions for the protection of personal data in **Union legal acts that entered into force on or before 6 May 2016** in the field of judicial cooperation in criminal matters and police cooperation, which regulate processing between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive, shall **remain unaffected**. (emphases added)

However, Article 62(6) LEDPD goes on to stipulates that, **by 6 May 2019**, the Commission must have **reviewed**:

> [all] other legal acts [i.e., other than the LEDPD itself] adopted by the Union which regulate processing by the competent authorities for the purposes set out in Article 1(1) including those referred to in Article 60, **in order to assess the need to align them**

[193] See Emilio De Capitani, o.c. (footnote 141, above).

> **with this Directive and to make, where appropriate, the necessary proposals to amend those acts** to ensure a consistent approach to the protection of personal data within the scope of this Directive. (emphasis added)

It follows from the above that **those 123 or so "other legal acts" do not need to be brought into line with the LEDPD by 6 May 2019**: all that is required is that they are ***reviewed*** by then, with a view to ***proposing*** changes to them where needed. **There is no set date for the making of the actual necessary amendments**, or even for the bringing forward of the relevant, detailed, instrument-by-instrument proposals.[194]

In the meantime, as Article 60 stipulates, the data protection rules in those 123 or so legal acts continue in force without change, and can be relied on as a basis for personal data transfers in the criminal law and public security area, even if they do not meet the requirements of the LEDPD – provided that **the three pre-conditions** for such transfers set out in the LEDPD are met: that the transfer is (in the view of the transferring EU entity) "necessary" for a criminal law or public security purpose; that the transfer is made to an authority in the third country with competence in these areas (unless that authority is ineffective or too slow or worse: violates human rights); and, if the transmitted data were originally obtained from a Member State, that that Member State authorised the transfer (or in urgent cases, was at least informed of it); and provided that ***either*** the relevant legal instrument contains "appropriate" data protection safeguards, ***or*** (if the instrument does not contain such safeguards) "*the transferring competent EU authority determines that fundamental rights and freedoms of the data subject concerned*" do not "*override the public interest in the transfer*".

Crucially, under the new "**accountability**" principle, **the assessments made by the entity** – i.e., as to whether the relevant legal instrument does contain "appropriate" data protection safeguards, or as to whether, and why, the public interest in the transfer outweighs the need to protect the fundamental rights and freedoms of the data subject – must now be **recorded** and, on request, made available to the European Data Protection Supervisor (and the Court).

Any DPO within a relevant competent EU entity must of course also play a major role in this: first of all, by alerting the organisation to the need to perform these tests, and thereafter, by internally verifying that those tests are applied, and are properly applied – and by consulting the European Data Protection Supervisor if needs be in case of internal disagreement or questions on these matters.

Delayed implementation in relation to treaties between EU Member States and third countries or international organisations:

As noted earlier, Article 61 stipulates that

> International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 6 May 2016 and which comply with Union law as applicable prior to that date shall remain in force until amended, replaced or revoked.

Transfers under any pre-May 2016 Member State – third country/international organisation treaty can therefore also continue for the time being,provided the three pre-

[194] At the time of the latest revision of this first edition of the handbook in early May 2019, no such proposals had yet been put forward by the Commission.

conditions for such transfers set out in the LEDPD are met: that the transfer is (in the view of the transferring authority) "necessary" for a criminal law or public security purpose; that the transfer is made to an authority in the third country with competence in these areas (unless that authority is ineffective or too slow or worse: violates human rights); and, if the transmitted data were originally obtained from another EU Member State, that that other state authorised the transfer (or in urgent cases, was at least informed of it); and provided that ***either*** the treaty contains "appropriate" data protection safeguards, ***or*** (if the treaty does not contain such safeguards) "*the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned*" do not "*override the public interest in the transfer*".

But again, under the "**accountability**" principle the assessments of the authority – i.e., as to whether the treaty does contain "appropriate" data protection safeguards, or indeed whether it meets pre-May 2016 Union law, or whether, and why, the public interest in the transfer outweighs the need to protect the fundamental rights and freedoms of the data subject – must now be **recorded** and, on request, made available to the supervisory authority (and the courts).

And also again, any DPO within a relevant competent authority in a Member State will have a major role to play in this.

Delayed implementation in relation to special Member States' automated processing systems in the criminal law and public security area

Article 63, which specifically deals with the transposition of the LEDPD into national law, stipulates in its first paragraph that:[195]

> Member States shall adopt and publish, by 6 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions. They shall apply those provisions from **6 May 2018**. (emphasis added)

In principle, it follows from this that the "laws, regulations and administrative provisions" in question had to brought into full compliance with the LEDPD by that date.

However, the article provides for the following **exception** in the next paragraph, subject toconditions:

> By way of derogation from paragraph 1, a Member State may provide, ***exceptionally, where it involves disproportionate effort***, for automated processing systems set up before 6 May 2016 to be brought into conformity with Article 25(1) by **6 May 2023**. (emphases added)

The third paragraph allows for yet longer delays, subject tofurther conditions:

> By way of derogation from paragraphs 1 and 2 of this Article, a Member State may, ***in exceptional circumstances***, bring an automated processing system as referred to in paragraph 2 of this Article into conformity with Article 25(1) **within a specified period** after the period referred to in paragraph 2 of this Article, ***if it would otherwise cause serious difficulties for the operation of that particular automated processing system***.

[195] The final, fourth, paragraph stipulates that: "*Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.*" The more specific stipulation in the first paragraph underlines that the full application of the LEDPD is in fact more a work to be progressed over several years, rather than a one-off transposition.

> The Member State concerned shall **notify the Commission** of the grounds for those serious difficulties and the grounds for the specified period within which it shall bring that particular automated processing system into conformity with Article 25(1). The specified period shall in any event not be later than **6 May 2026**. (emphases added)

All the above does mean that the full application of all the requirements of the LEDPD, including in particular those relating to data transfers to third countries and international organisations, will still take some time.

However, in the meantime it is worth recalling that under the Directive (contrary to the situation under the previous Council Framework Decision) compliance by the Union and Member States' rules and actions relating to criminal and public security matters are now justiciable. This includes, ultimately, the verification of whether any such rules and actions comply with the LEDPD – including whether the above-mentioned tests (whether a treaty contains "appropriate" data protection safeguards or meets pre-May 2016 Union law; or whether in a specific case the public interest in the transfer really outweighed the need to protect the fundamental rights and freedoms of the data subject(s)) are met; and, in relation to any delay in bringing the above-mentioned operations in line with the Directive, whether the special conditions for such delays, set out in the paragraphs quoted above are met.

1.4.4 New data protection instruments in the Common Foreign and Security Policy (CFSP) area

As the Commission explains:[196]

> The 2009 Lisbon Treaty did much to strengthen the Union's activities in the area of external action. First, it created the post of **High Representative (HR) of the Union for Foreign Affairs and Security Policy**. …
>
> And, second, the Treaty established the **European External Action Service (EEAS)**. Operational since 2011, it is essentially the EU's new diplomatic service, assisting the HR in the conduct of EU foreign policy. Notably, the EEAS runs the network of **141 EU Delegations** around the world.
>
> The EEAS works to ensure the consistency and coordination of the Union's external action, preparing policy proposals and implementing them after their approval by the European Council. …
>
> Alongside the EEAS, a new Commission service, the service for **Foreign Policy Instruments (FPI)**, was set up to take over responsibility for operational expenditure.
>
> Today, under the authority of [the HR], and working very closely with the EEAS and EU delegations, the FPI is tasked with … implementing the Common Foreign and Security Policy (CFSP) budget [and a variety of other instruments and actions]. …[197]
>
> The budget for the wide range of FPI-managed activities amounts to EUR 733 million in 2014.

The work done by the HR, the EEAS and the staff of the FPR service will often involve the processing of personal data, e.g., in relation to the imposition of sanctions on individuals, or

---

[196] See: https://ec.europa.eu/fpi/about-fpi_en

[197] For a list with links to each specific instrument or action, see the webpage referred to in the previous footnote.

the freezing of their assets.[198]

However, such processing is not subject to the same EU treaty rules as is the processing by entities subject to the GDPR, the LEDPD or even the other EU institutions. All those others are covered by the general guarantee of personal data protection enshrined in Article 16 TFEU:

Article 16

1. Everyone has the right to the protection of personal data concerning them.
2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

However, this does not apply to processing of personal data by the CFSP bodies mentioned above because after the above, the last sentence in Article 16 TFEU stipulates that:

> The rules adopted on the basis of this Article shall be **without prejudice to thespecific rules** laid down in **Article 39** of the Treaty on European Union.

The latter article in the TEU stipulates the following:

Article 39

> In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, **the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter**[i.e., in relation to the CFSP], and the rules relating to the free movementof such data. Compliance with these rules shall be subject to the control of independent authorities.

This is not the place to discuss these matters further.[199] Suffice it to note that in the area of CFSP, the regulation covering processing of personal data by the EU institutions (etc.), Regulation 2018/1725, discussed in the next section, applies – but only to a limited extent; and that, in order to know the specific data protection rules relating to each data processing activity inthe context of the CFSP, including which data protection authority is competent for what, and whether a DPO must be designated, it is necessary to know the particular Council decision related to it.

---

198 Cf. the opinions and comments of the EDPS on such matters, listed here: https://edps.europa.eu/data-protection/our-work/subjects/common-foreign-and-security-policy_en

199 For further discussion, see:

- EDPS letter of 23 July 2007 to the IGC presidency on data protection under the Reform treaty (as the Lisbon Treaty was called during its drafting).
- EDPS, Joint Opinion on the notifications for Prior Checking received from the Data Protection Officer of the Council of the European Union regarding the processing of personal data for restrictive measures with regard to the freezing of assets, Brussels, 07 May 2014 (2012-0724, 2012-0725, 2012-0726), p. 10, available at: https://edps.europa.eu/sites/edp/files/publication/14-05-07_processing_personal_data_council_en.pdf

1.4.5 Data protection for the EU institutions: a new regulation

As noted in section 1.3.6, above, the first EU instrument on data protection in relation to processing of personal data by the EU institutions themselves, Regulation 45/2001, was repealed by Regulation (EU) 2018/1725, which entered into force in **11 December 2018**[200](but with some **exceptions** and some **delays in application**, as noted under those headings below).

Two regimes

Those exceptions and delays aside, Regulation 2018/1725 actually creates **two separate data protection regimes**: one for all the ***EU institutions and bodies not involved in police and judicial cooperation***, and one for the ***EU institutions and bodies that are involved in such cooperation*** (see Art. 2, paras. (1) and (2))

- **The data protection regime applicable to EU institutions and bodies not involved in police and judicial cooperation:**

This regime, set out in Chapters I to VIIIof the new regulation, is **largely the same as the regime established by the General Data Protection Regulation (GDPR)** for processing subject to that latter instrument. Thus, Regulation 2018/1725, like the GDPR, includes the new "**accountability**" principle (Art. 4(2); cf. also Art. 26) and sets out the **obligations of controllers and processors(Chapter IV), in effectively the same terms as those of controllers and processors subject to the GDPR.**

Specifically, Chapter IV includes provisions on the principle of "**data protection by design and default**" (Art. 27); on the arrangements to be put in place in relation to "**joint controllers**" (Art. 28), **processors** (Art. 29) and **persons acting under the authority of the controller or processor** (Art. 30); on the ("accountability"-related) duty to keep detailed **recordsof processing activities** (Art. 31); on **security of processing** (Art. 33), **notification of data breaches** to the**European Data Protection Supervisor (EDPS)** (which is the supervisory authority in relation to the EU institutions and bodies) (Art. 34) and **communication of data breaches to data subjects** (Art. 35) – all on the same lines as the GDPR.

Regulation 2018/1725 (like its predecessor, Regulation 45/2001, discussed in section 1.3.6, above) requires each Union institution or body to appoint a **Data Protection Officer (DPO)** (Art. 43) – which is again also in line with the requirement in the GDPR in relation to public sector controllers. The provisions on **the position of the DPO** (Art. 44) and on the **tasks of the DPO** (Art. 45) are also in line with the GDPR, with ***some additional stipulations*** on access to the DPO by anyone and protection against prejudice for doing so (Art. 44)(7) and on the term of appointment of a DPO (Art. 45(8)); and in relation to the DPO's task, a somewhat stronger stipulation (not found in the GDPR) that the DPO shall "*ensure in an independent manner the internal application of this Regulation*" (Art. 45(1)(b)).[201]

---

[200] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21 November2018, p. 39–98, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725

[201] This is stronger because, although the GDPR stipulates that "*[t]he controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks*" and that "*[h]e or she shall not be dismissed or penalised by the controller or the processor for performing his*

Regulation 2018/1725 also requires the carrying out of a **Data Protection Impact Asssessment (DPIA)**, in the same circumstances as provided for in the GDPR, i.e., in relation to processing "likely to result in a high risk to the rights and freedoms of natural persons" (Art. 39); and stipulates that there must be "**prior consultation**" with the EDPS in similar circumstances as stipulated for prior consultation with the relevant supervisory authority in the GDPR, i.e., if the DPIA indicates that those risks cannot be sufficiently mitigated (Art. 40) (The last sentence of Art. 40 usefully adds that "*The controller shall seek the advice of the data protection officer on the need for prior consultation*" – but that is of course advisable in relation to processing under the GDPR too.)

As to substantive content, Regulation 2018/1725 also rests on the same ***definitions***(Art. 3) and ***core principles***(Art. 4) as the GDPR, and contains effectively the same rules on issues such as ***consent and other legal bases for processingof non-sensitive and sensitive data*** (cf. Arts. 5 – 13), but with some further detail on "***compatible processing***" (Art. 6) and on ***transmissions of personal data to recipients in the Member States*** (Art. 9);[202]and ***data subject rights*** (Arts. 14 – 24), including in relation to the taking of ***fully automated decisions and profiling*** (Art. 24).

It also provides for essentially the same permissible ***restrictions on data subject rights and on the duty to communicate a personal data breach to the data subject*** (Art. 25(1)), but extends these also to ***the duty to ensure the confidentiality of electronic communications*** (noted below) and, more important, lays down more specific rules on what any "***legal act or internal rule***" providing for such restrictions should specifically clarify (see Art. 25(2)). Moreover, the European Data Protection Supervisor must be consulted on the drafts of such rules (Art. 41(2)), which constitutes a significant guarantee that they will indeed be limited to what is "*necessary and proportionate … in a democratic society*".

Regulation 2018/1725 includes a special section (Chapter IV, section 3) on **confidentiality of electronic communications**. This stipulates that

> Union institutions and bodies shall **ensure the confidentiality of electronic communications**, in particular by securing their electronic communications networks (Art. 36, emphasis added) –

and that they shall:

> **protect** the information transmitted to, stored in, related to, processed by and collected from the terminal equipment of users accessing their publicly available websites and mobile applications, in accordance with Article 5(3) of Directive 2002/58/EC [i.e., the e-Privacy Directive, discussed in section 1.3.3, above] (Art. 37, emphasis added).

The final article in this section concerns **directories of users**, as defined in Article 3(24), i.e. any:

---

tasks" (Art. 38(3) GDPR), which effectively ensures that the DPO can act in "an independent manner", the GDPR says that the DPO must "*monitor compliance with [the GDPR and other relevant rules]*" and "*inform and advise*" the controller and its employees (and any processors) of their obligations (Art. 39(1)(b) and (a), respectively), the GDPR does not require the DPO to "*ensure*" internal compliance, the legal responsibility remaining to the controller.

[202] See sub-section 1.4.6, below.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

> publicly available directory of users or an internal directory of users available within a Union institution or body or shared between Union institutions and bodies, whether in printed or electronic form.

Article 38 stipulates in this regard that the personal data contained in such directories must be "*limited to what is strictly necessary for the specific purposes of the directory*" (Art. 38(1)), and that the institutions and bodies must:

> take all the necessary measures to prevent personal data contained in those directories from being used for direct marketing purposes regardless of whether they are accessible to the public or not.

The rules in this section reflect some of the rules in the e-Privacy Directive, discussed in section 1.3.3, above.

The rules on **transfers of personal data to third countries or international organisations**, contained in Chapter V of Regulation 2018/1725 again follow the same scheme as is contained in the GDPR: such transfers may only take place:

- on the basis of an **adequacy decision** issues by the Commission under the GDPR; or
- if "**appropriate safeguards**" are provided by means of:
  - a legally binding and enforceable instrument between public authorities or bodies;
  - standard data protection clauses adopted by the Commission;
  - standard data protection clauses adopted by the EDPS and approved by the Commission;
  - in relation to transfers to a processor who is not a Union institution or body: Binding Corporate Rules (BCRs), codes of conduct or certifications issued under the GDPR; or

  subject to the authorisation of the EDPS:
  - contractual clauses between the relevant entities; or
  - data protection provisions inserted in administrative arrangements (agreements) between public authorities or -bodies.

  (Art. 48)

Regulation 2018/1725 also contains the stipulation, identical to the one in the GDPR, that:

> Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement. (Art. 49)

Finally, in this respect, Article 50 of Regulation 2018/1725 provides for transfers on the basis of "**derogations for specific situations**", on the same lines as those set out in the GDPR, i.e., when the data subject has "**explicitly consented**" to the proposed transfer (Art. 50(1)(a)), or when the transfer is "**necessary**" in a ***contractual context*** (Art. 50(1)(b) and (c)), for ***important reasons of public interest recognised in Union law*** (Art. 50(1)(d) read with Art. 50(3)), for the establishment, exercise or defence of ***legal claims*** (Art. 50(1)(e), or to protect the ***vital interests of the data subject or of other persons***, where the data subject is

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

physically or legally incapable of giving consent (Art. 50(1)(f); or when the transfer is made from a **publicly accessible register** (provided the conditions for access are met) (Art. 50(1)(g)).

Regulation 2018/1725, like the GDPR in relation to public authorities, stipulates that the first three of these special derogations (explicit consent of the data subject; contractual contexts) "*shall not apply to activities carried out by Union institutions and bodies in the exercise of their public powers*" (Art. 50(2)).

Chapter VI of Regulation 2018/1725 covers **the establishment, rules, position, tasks and duties of the EDPS**.Essentially, the EDPS fulfils in relation to the processing of personal data by the Union institutions and bodies the same function as the supervisory authorities (data protection authorities, DPAs) established under the GDPR fulfil in relation to processing of personal data by the relevant national public authorities in the Member State (or region of a Member State) for which they are competent.

Chapter VII covers **cooperation between and coordinated supervisionby the European Data Protection Supervisor and national supervisory authorities**.The Regulation also, again like the GDPR, **encourages cooperation with third countries and international organisations** for the protection of personal data (Art. 51).[203]

Finally, Chapter VIII deals with **remedies, liability and penalties**, which again are similar to those required under the GDPR. Suffice it to note that any data subject whose personal data are or have been processed by an EU institution or body may lodge a complaint with the EDPS (Art. 63) (just as any data subject can complain under the GDPR to the relevant national DPA) and (again as under the GDPR) is entitled to compensation for any material or non-material damage caused by any infringement of the Regulation (Art. 65). Moreover, as under the GDPR, data subjects can in such cases be represented by not-for-profit organisations active in relation to personal data (Art. 67) – to which the Regulation adds a further provision on complaints by EU staff (Art. 68). Conversely, any EU official who fails to comply with the obligations imposed by the Regulation is liable to disciplinary action (Art. 69).

The Court of Justice of the EU has jurisdiction over any dispute relating to the Regulation, including in relation to compensation (Art. 64). And **the EDPS can impose administrative fines** on Union institutions and bodies that fail to comply with the Regulation (Art. 66) (although the level of fines is much lower than the level provided for in the GDPR).[204]

---

[203] As in the GDPR, the relevant provision (Art. 50 in the GDPR) is somewhat oddly placed in the chapter dealing with data transfers rather than in the one on the tasks and powers of the supervisory authorities.

[204] The maximum fines that the EDPS can impose on EU institutions or bodies for non-compliance with Regulation 2018/1725 are, respectively, €25.000 per infringement and up to a total of €250.000 per year for some infringements, and €50.000 per infringement and up to a total of €500.000 per year for some other infringements (see Art. 66(2) and (3)). This compares to administrative fines up to €10.000.000, or in the case of an undertaking (private company), up to 2% of the total worldwide annual turnover (whichever is higher) for some infringements, and up to €20.000.000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover (whichever is higher) for some other infringements, that can be imposed under the GDPR (Art. 83(4) and (5)) – although the GDPR also allows the Member States to reduce these amounts or even to fully exclude public authorities and bodies established in their territory from administrative fines altogether (Art. 83(7) (but such authorities exempt from fines or subject to reduced fines must still remain subject to the powers of the relevant DPAs under Article 58(2) GDPR).

Given that the main data protection regime under Regulation 2018/1725 is so closely aligned with the GDPR, the – often very detailed and practical – guidance and views issued by the European Data Protection Supervisor to the EU institutions and bodies subject to this regime will also be of direct importance to controllers processing personal data under the GDPR, especially in the public sector, and should therefore be carefully studied by any DPO working for such a controller (together, of course, with the guidance and opinions of the European Data Protection Board, of which the EDPS is a member: the views of the EDPS and the EDPB feed into each other).

- **The data protection regime applicable to EU institutions and bodies that are involved in police and judicial cooperation:**

General:

As noted above, Regulation 2018/1725 creates **a separate data protection regime for EU institutions and bodies that are involved in police and judicial cooperation** (i.e., that are involved in "*activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU*"). This separate regime is set out **in Chapter IX of the Regulation**, comprising Articles 70 to 95 (whereby Article 2(2) makes clear that the **definitions** set out in Article 3 also apply to this chapter).[205]

The special regime regulates the processing by the relevant institutions or bodies of "**operational personal data**". These are defined in Article 3(2) as:

> all personal data processed by Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU to meet the objectives and tasks laid down in the legal acts establishing those bodies, offices or agencies.

Basically, processing of such **operational personal data** is subject to the special regime in Chapter IX, while processing of all "non-operational" personal data – such as human resource data relating to the staff of the relevant institutions and bodies – is subject to the main regime set out in the earlier chapters of Regulation 2018/1725, as described under the previous sub-heading.

Under that previous sub-heading, we noted that the rules for the main regime are closely aligned with the GDPR. Similarly,the rules in Chapter IX of Regulation 2018/1725 are often in line with the Law Enforcement Data Protection Directive (LEDPD), discussed in section 1.4.3, above(or with both that directive and the GDPR and the rules for the main regime under Regulation 2018/1725) – but Chapter IX is not quite as closely aligned with the LEDPD as the main regime is with the GDPR.The matters can be quite intricate.[206]

Given that this handbook is aimed at DPOs in public bodies in the Member States, the

[205] On the question of whether, and if so to what extent, Chapters VII and VIII apply to processing under Chapter IX, see below, under the headings "*Rights, supervision and Enforcement*".

[206] To give just one example: closely related to the new "accountability" principle that applies to all the modern EU data protection instruments, is the duty of controllers to keep **records** and **logs**. However, the GDPR and the rules applying to the main regime under Regulation 2018/1725 both require the keeping of detailed records of all processing operations (Art. 30 GDPR; Art. 31 of Regulation 2018/1725), but do not require the keeping of logs. The LEDPD requires both detailed records and details logs (Arts. 24 and 25). But Chapter IX of Regulation 2018/1725 only requires logs to be kept in relation to the processing of operational personal data (Art. 88), without mentioning records.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

details of the correspondence or divergence between the rules in Chapter IX and those in the earlier part of Regulation 2018/1725 – and those in the main EU data protection instruments, the GDPR and the LEDPD – need not be discussed here. Two special matters may however be noted under the next sub-headings.

Rights, supervision and enforcement:

There are **no references** in Chapter IX to the data subject's right to ***compensation for damage caused by wrongful processing*** (which *in casu* would mean processing contrary to the provisions of that chapter), to the right of data subjects to be ***represented*** by a not-for-profit body, or to the power of the EDPS to impose ***administrative fines***.

The provisions of Chapter IX do repeatedlymentionan obligation on the part of a controller subject to Chapter IX to **informdata subjects** of their ***right to lodge a complaint with the EDPS*** (see Arts. 79(1)(d), 80(f) and 81(2)) and indeed of the possibility of seeking ***a judicial remedy before the Court of Justice*** (Art. 81(2). Controllers subject to Chapter IX may also arrange for the **rights of data subjects** in some cases to be "*exercised through the European Data Protection Supervisor*" (Art. 84(1), i.e., only indirectly; and in those case, too, they must:

> **inform the data subject of the possibility of exercising his or her rights through the European Data Protection Supervisor** pursuant to paragraph 1. (Art. 84(2))

The controller must also make the **logs** of its processing operations **available to the EDPS** onrequest (Art. 88(3)) and **report personal data breaches to the EDPS** (Art. 92(1) and (4)).

However,it clearly follows from Article 2(2) thatthe chapter in the Regulation that actually provides for thehandling of complaints by the EDPS and the jurisdiction of the Court of Justice of the EU, and for enforcement action by the EDPS, also in cases of personal data breaches (Chapter VIII), and the chapter that actually spells out the tasks and powers of the EDPS in these regards (Chapter VI), do not apply to processing of operational data which is subject to Chapter IX only.

It would appear that, in practice, the EDPS does assume supervisory and advisory powers, also in relation to the processing of operational personal data by EU institutions and bodies under Chapter IX of Regulation 2018/1725, and will be willing to accept complaints from data subjects in relation to such processing. Whether he will allow data subjects to be represented by NGOs in such cases, or would be willing to order compensation, or even impose administrative fines on the relevant institutions and bodies – and whether the Court of Justice would endorse such exercise of the EDPS's powers in relation to such processing – remains to be seen.

Exceptions from and delayed implementation of Regulation 2018/1725

In principle, Regulation 2018/1725 applies to ***all the processing of personal databy all Union institutions and bodies*** (Art. 2(1)) – albeit, as we have seen, by creating two distinct legal regimes. However, the Regulation also contains some exemptions from its application, and provides for delayed implementation of its provisions in some other contexts, as discussed next.

- **Exemptions:**

Article 2(4) stipulates that:

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

> **This Regulation shall not apply to the processing of personal data by missions referred to in Articles 42(1), 43 and 44 TEU.** (**E**mphasis added)

The missions and tasks covered by the exemption are:

- missions outside the Union for peace-keeping, conflict prevention and strengthening international security in accordance with the principles of the United Nations Charter (Art. 42(1)); and
- joint disarmament operations, humanitarian and rescue tasks, military advice and assistance tasks, conflict prevention and peace-keeping tasks, tasks of combat forces in crisis management, including peace-making and post-conflict stabilisation. All these tasks (Art. 43, on which Art. 44 expands).

The second sentence of Article 43 adds that all the operations and tasks mentioned in that article "*may contribute to the fight against terrorism, including by supporting third countries in combating terrorism in their territories*".

- **Delayed implementation:**

Apart from the above-mentioned exclusion of the application of the Regulation in relation to specific operations for which specific rules may be specified, the Regulation also sets outthe processes for bringing the processing operations of some other EU institutions and bodies into line with Regulation 2018/1725, with deadlines for the relevant reviews (but not for the actual bringing in line of these operations with the Regulation). Specifically, first of all, Article 2(3) stipulates that:

> This Regulation shall not apply to the processing of operational personal data by **Europol** and the **European Public Prosecutor's Office**, until [the pre-Lisbon regulations that cover their activities][207] are adapted in accordance with Article 98 of this Regulation. (emphases added)

Moreover, Article 98 stipulates that:

> 1. **By 30 April 2022**, the Commission shall **review** legal acts adopted on the basis of the Treaties which regulate the processing of operational personal data by Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU [i.e., which relate to police or judicial cooperation], in order to:
>
> (a) **assess** their consistency with [the Law Enforcement Data Protection Directive (as discussed in section 1.4.3, above)] and Chapter IX of this Regulation;
>
> (b) **identify** any divergences that may hamper the exchange of operational personal data between Union bodies, offices or agencies when carrying out activities in those fields and competent authorities; and
>
> (c) **identify** any divergences that may create legal fragmentation of the data protection legislation in the Union.

[207] Respectively: Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24 May 2016, p. 53, and Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), OJ L 283, 31 October 2017, p. 1.

> 2. On the basis of the review, in order to ensure uniform and consistent protection of natural persons with regard to processing, **the Commission may submit appropriate legislative proposals, in particular with a view to applying Chapter IX of this Regulation to Europol and the European Public Prosecutor's Office** and including adaptations of Chapter IX of this Regulation, if necessary.
>
> (emphases added)

In other words, the regulations covering **the work of Europol and the EPPO**, and of any other institutions and bodies covered by Article 98,must be ***reviewed*by30 April 2022**, and the Commission may then ***propose*** new rules with a view to bringing the processing of personal data by these bodies into line with the LEDPD (discussed in section 1.4.3, above) and with the special rules in Chapter IX of the Regulation (discussed above). However, **no date** is set for the actual adoption of such new rules, which will require legislative action by the Council of Ministers and possibly the new European Parliament, and the obtaining of opinions from the European Data Protection Supervisor and the European Data Protection Board – which will all take some time. Until those regulations are amended to these ends – i.e., at least for the next few years – the processing of personal data by Europol and EPPO (and any other institutions or bodies covered by Article 98 of Regulation 2018/1725) will remain under their own, current (pre-2018) data protection rules.

1.4.6 Transmissions of personal data between different EU data protection regimes

i. The different data protection regimes

It will be clear from the various earlier sections that there are, in fact, a considerably number of **different,general or more specificdata protection regimes within the main EU data protection instruments and frameworks**, and **some more outside of those** (and even **outside of EU law altogether**), including those set out below. Which regime applies to a particular activity or processing operation will depend on the assessment of each such activity or operation and its specific purpose, in particular whether the matter falls within EU competence or not, whether it takes place in the private or public sector, whether it involves EU- or national institutions acting in relation to economic or criminal matters, etcetera.

General Data Protection Regulation:

- The GDPR regime as applied to processing by private entities.
- The GDPR regime as applied to processing by public entities not involved in criminal-legal- or public security- or national security matters (or when not involved in such matters) (whereby "public security" must be read as a very limited category).

e-Privacy Directive/proposed e-Privacy Regulation:

- The specific rules applied to e-communication service providers (and in future to other providers such as "Over-The-Top" players).
- The specific rules applicable to all webhosts (including public authorities with their own webpages) in relation to confidentiality of communications, the use of "cookies", etc..

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Law Enforcement Data Protection Directive:

- The LEDPD as applied to public entities ("competent authorities") when they process personal data "*for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*", either as their main task or occasionally, aside from other public tasks.

Areas exempt from the LEDPD (for the time being):

- The rules in the approximately 123 EU legal instruments relating to what used to be called "Justice and Home Affairs" (JHA) matters that entered into force before 6 May 2016 (which continue to apply even if they do not yet conform to the LEDPD).
- The rules in "*international agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 6 May 2016 and which comply with Union law as applicable prior to that date*" (which also continue to apply even if they do not yet conform to the LEDPD).
- The rules on the use of "*automated processing systems set up before 6 May 2016*" in the Member States, if they have not yet been brought into line with the LEDPD because that would have involved a "*disproportionate effort*".

Processing of personal data in the CFSP area:

- Processing by the EU High Representative for Foreign Affairs and Security Policy, the European External Action Service (EEAS) and the 141 EU Delegations around the world, and the service for Foreign Policy Instruments (FPI) and processing by the Member States in relation to these matters (including in relation to the adoption of Council Decisions in the CFSP area) – *which are not yet subject to any specific EU data protection instrument*. [But note the third indent under the next heading]

Processing of personal data by the EU institutions or bodies under Regulation 2018/1725:

- The data protection regime applicable to EU institutions and bodies not involved in police and judicial cooperation.
- The data protection regime applicable to EU institutions and bodies that are involved in police and judicial cooperation.
- Processing by the Council Secretariat in implementing CFSP Council Decisions – the limited area of activity relating to CFSP that is subject to data protection rules, i.e., to Regulation 2018/1725.

Areas exempt from Regulation 2018/1725 (for the time being):

- Processing of personal data by EU missions aimed at **peace-keeping**, conflict prevention and strengthening international security, or charged with joint **disarmament operations**, **humanitarian and rescue tasks**, military advice and assistance tasks, **conflict prevention and peace-keeping tasks**, tasks of **combat forces in crisis management**, including peace-making and **post-conflict stabilisation** (including when such tasks relate to the fight against terrorism, including by supporting third countries in combating terrorism in their territories).

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

- Processing of personal data by Europol and the European Public Prosecutor's Office (EPPO) and other "*Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU [i.e., which relate to police or judicial cooperation]*", which will continue to take place on the basis of the EU legal instruments relating to Europol or EPPO or otherwise to police or judicial cooperation, adopted prior to Regulation 2018/1725.

National security:

- Processing of personal data by Member States in relation to national security – **which is altogether outside of the scope of EU law**, indeed even of the Charter of Fundamental Rights(although such processing is of course subject to the European Convention on Human Rights and the jurisdiction of the European Court of Human Rights).[208]

It is not always easy to draw clear lines between these many different regimes, e.g., between police action against crime, police action to secure order, police and other authorities' actions to ensure "internal security", "public security" and "national security", and between those actions and the actions of the EU in relation to "terrorism",[209] the above-mentioned tasks of EU missions, and "international security".

This is not the place to explore these distinctions in depth. Suffice it to note that, when different regimes apply to the different activities (activities falling within more than one of the above categories), perhaps even by the same actors, it will be important for the relevant actors, as controllers (and often also as processors, e.g., when supporting other such actors) to **clarifyfor themselveswhich legal regime applies to which personal data processing operation, and to what personal data, by analysing each specific data processing operation in question.** The legality of the processing and the scope of and exceptions to such important matters as data subject rights, always crucially depend on such clarifications.

Public authorities involved in different activities that are subject to different data protection regimes should always carefully distinguish their different activities, different processing operations, and different personal data used for the different operations in their personal data processing records and in their assessments of such processing.[210] **Data Protection Officers in such public bodies will have to play a crucial role in that regard.**[211]

---

[208] The European Court of Human Rights has issued several important judgments in this respect. See: European Court of Human Rights Research Division, *National security and European case-law*, Council of Europe, 2013, available at:
https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf
However, these cannot be applied by the EU institutions in relation to such activities.

[209] Cf. John Vervaele, *Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?*in: Utrecht Law Review, Volume 1, Issue 1 (September 2005), available at:
http://www.utrechtlawreview.org/

[210] Cf. Article 74 of Regulation 2018/1725 on making a "*[d]istinction between operational personal data and verification of the quality of operational personal data*", which is a good example of what should be general good practice whenever a controller is engaged in activities subject to different data protection regimes.

[211] See Part Three of this handbook.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

ii. Transmissions of personal data

Special issues arise when it is proposed or requested that personal data that were obtained for one particular purpose under the rules in one of the above-mentioned legal regimes be used by the same controller for a different purpose, for processing under a different legal regime; or be transmitted or otherwise made available to another body (another controller) for such a different purpose, for processing under a different legal regime.[212]

For example, the educational department in a local authority may collect personal data on schoolchildren for educational purposes, under the GDPR, but may be asked by its local police agency for access to (some of) those data, to help in solving local crime (e.g., to check which children had been absent from school on a particular day). The proposed processing of the data for the second purpose would be under the LEDPD (or to be more precise, the national-legal provisions transposing the LEDPD, as well as under relevant police- or criminal procedure law). Sometimes, the applicable laws or legal rules clarify when such disclosures can take place (e.g., only in relation to certain crimes, or only if there was reasonable suspicion against identified children, or only if a judge issued a warrant). But often, this will be a matter to be decided by the relevant local authority in the light of the rules in the various applicable instruments. **The local authority's DPO will have an important role in advising on this matter (and should consult the DPA if in any doubt).**

Regulation 2018/1725 provides some guidance on transmissions of personal data by an EU institution or body to "*recipients established in the Union other than Union institutions and bodies*" – typically, public authorities of the Member States. EU institutions and bodies are allowed to transmit data to an entity in a Member State requesting the data provided that:

> (a) the recipient [i.e., the entity in a Member State requesting the data] establishes that the data are necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the recipient [i.e., in that entity]; or
>
> (b) the recipient establishes that it is necessary to have the data transmitted for a specific purpose in the public interest and the controller [i.e., the EU institution or body asked to provide the data], where there is any reason to assume that the data subject's legitimate interests might be prejudiced, establishes that it is proportionate to transmit the personal data for that specific purpose after having demonstrably weighed the various competing interests.
>
> (Art. 9(1))

EU institutions or bodies are allowed to transmit (send) such data to entities in Member States without being asked, i.e., of their own motion, if they can:

> demonstrate that the transmission of personal data is necessary for and proportionate to the purposes of the transmission by applying the criteria laid down in points (a) or (b) of paragraph 1.
>
> (Art. 9(2))

[212] Note that the data transmissions discussed here are different from transmissions of personal data by one entity to another entity in the same country or another Member State for the same purpose, under the same [EU] data protection regime – e.g., by one law enforcement agency in one Member State to another LEA in that Member State or to an LEA in another Member State; and from transfers of personal data to third countries (which are subject to the special rules on such transfers – but note that those too differ between the different regimes).

But several matters must be taken into account in that respect. First of all, the above applies to EU institutions and bodies not involved in processing in relation to police and judicial cooperation, i.e., it applies only to processing – and transmissions – under the "main regime" established by Regulation 2018/1725 for EU institutions and bodies; and as noted in section 1.4.5, above, that "main" data protection regime in that regulation is closely aligned with the GDPR. There is no corresponding provision on transmissions of personal data to bodies in the Member States in Chapter IX of Regulation 2018/1725, which covers processing of "operational" personal data by EU institutions and bodies that are involved in police and judicial cooperation.

Secondly, the rules in Article 9, quoted above, are "without prejudice" to the core data protection principles, including purpose-limitation and the rule on "compatible" processing (see Art. 6 of the Regulation which adds significant conditions to that), data relevance, etc., and to the stipulations on lawful processing (see the introductory clause to Article 9(1)). They are also without prejudice to the special rules on the processing of sensitive personal data (*idem*).

Still, Article 9 of Regulation 2018/1725 illustrates that **whenever personal data that are processed under one of the above-mentioned regimes are to be transmitted to another entity (or even used by the same entity) for processing under another regime, important questions about purpose-specification, relevance and adequacy of the data, and about the lawfulness, necessity and proportionality of the change in purpose must be addressed.**

In that regard, it is crucial to remember, first of all, that "transmitting" data, like any other form of "disclosure" of personal data (including "making [personal data] available", e.g., online) constitutes a form of processing (see Art. 4(2) GDPR, repeated *verbatim* in all the other EU data protection instruments). Secondly, crucially, any "transmission" of personal data between different entities always has two aspects:

- for the transmitting entity, it is a form of **disclosure** of the data (see above); but
- for the receiving entity, it constitutes **collecting** of personal data – which is a separate act covered by the general concept of "processing", distinct from "disclosure", "transmission" or "making available" of personal data.

If, in relation to their respective activities relating to the transmission of the data, the two entities are subject to different data protection regimes, each should assess the compatibility of its relevant action with the data protection rules that apply to it.

Thus, in the above example, the local educational department will be subject to the GDPR and to any "further specifications" on how the GDPR provisions are to be applied, set out in the relevant national data protection law (or perhaps in an appropriate data protection section of the law on the tasks and powers of local educational departments, which should still be in line with the GDPR).

On the other hand, the local police agency will be subject to the national legal provisions adopted to implement the LEDPD (as well as to any relevant rules in the national police- or criminal procedure laws, which should be in line with the LEDPD).

In that case, the local educational department must check (with the help of its DPO and if needs be with advice from the relevant DPA) whether the data protection rules to which it is

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

subject allow it to disclose the personal data to the police agency (or not, or subject to what conditions).

Conversely, the local police agency should, before making the request for the data to the educational department, check (with the help of its DPO and if needs be with advice from the relevant DPA) whether the data protection rules to which it is subject allow it to request or demand the personal data from the local educational authority (or not, or subject to what conditions).

It will often be useful for the two DPOs to discuss these matters between them (and consult the DPA jointly where appropriate).

Often, the relevant rules will be mutually compatible and actually cross-refer to each other. For instance, the police law may provide when, and subject to what conditions, the local police agency may ask "other public authorities" for information (generally, and/or on children); and the rules applicable to the educational department may stipulate that the department may – or must – provide information requested by "another public authority" (or specifically by the police), provided that the request is lawful. That would still require the police agency to follow the rules and meet the relevant conditions, and the educational department to at least ask for assurances (and proof) that the request made by the police is lawful and meets the relevant conditions. But those matters aside, there are no problem as regards the transmission of the data.

When both the transmitting agency and the requesting agency are subject to the latest EU data protection rules described above – in particular, the GDPR, the LEDPD and Regulation 2018/1725 – there should usually be no problems in these regards (although individual cases may still require serious analysis and attention).

The issues are less clear-cut when one entity – in particular a requesting entity – is not subject to the latest rules, but still only to less demanding legacy rules – although these will still at least be basedon the general data protection principles underpinning all EU data protection law.

However, the matters may in practice be seriously complicated when a requesting entity is not subject to any appropriate data protection rules at all – as is the case, as we have seen, in relation to CFSP matters, matters relating to EU peace-keeping or other military missions, or national security. In this context, "appropriate" rules are rules that are clearly based on and acknowledge the general data protection principles; that depart from the ordinary rules built on those principles only to the extent specifically stipulated in a relevant (publicly available, clear and precise) legal instrument that is "foreseeable" in its application, and only to the extent "strictly necessary" for the relevant purpose, with any such departures clearly "proportionate" to the special context;[213] and that provide for control over compliance with the special rules by an independent authority.[214]

This is not the place to discuss this in detail. But some broad points may be made.

[213] These are the rule of law requirements developed by the European Court of Human Rights and equally applied by the Court of Justice of the EU and reflected in the EU Charter of Fundamental Rights (CFR), that must be adhered to by any democratic state in any activity that may impact on the fundamental rights and freedoms of the individual.

[214] As expressly provided for in Art. 8(3) CFR.

Thus, any transmission of personal data by a national public authority (or an EU institution or body) that is subject to the latest EU data protection rules (i.e., the GDPR, the LEDPD or Regulation 2018/1725) to any national or EU entity that is not subject to any appropriate data protection law at all is potentially as erosive of EU data protection as any transfer of such data to a country without appropriate ("adequate") data protection rules – which is in principle prohibited, unless "appropriate safeguards" are adopted (cf. Chapter V of the GDPR).

Entities subject to any of the above-mentioned latest EU data protection instruments should therefore be careful before providing personal data that they process subject to those instruments to a requesting entity that is not subject to any appropriate data protection rules. They should carefully check – as always, with the help of their DPO and if needs be by consulting the relevant DPA – whether the instrument that applies to them allows such a transfer (at all) or prohibits it or imposes conditions on it; and they should refuse to transmit the data unless this is allowed under the instrument that applies to them, in sufficiently clear terms.

It is not sufficient for a requesting entity that is not subject to appropriate data protection rules to point out to the requested entity that it (the requesting entity) is allowed to obtain (collect) the data it is asking for under the rules that apply to that requesting agency: that may legitimise the data collecting in terms of those rules, but it does not legitimise the data disclosure ("transmission") by the requested entity under the data protection rules that apply to the requested entity (especially if those rules are set out in or adopted under the above-mentioned latest EU data protection instruments).

Sometimes, states have still in place laws that give some of their agencies – in particular, their **intelligence agencies** – the right to demand information, or access to information, including personal data, in the broadest of terms; and sometimes, the laws are framed in such a way that they override any restrictions on the disclosure of personal information by other entities that are subject to data protection laws, and which (the over-broad laws stipulate) must comply with such demands irrespective of what the relevant data protection rules that normally apply to them say. This includes laws in Member States.[215]

In respect of national security agencies, the relevant Member State may argue that the rules under which those agencies may demand information (or access to databases) are outside the scope of EU law – and that the transmission of data to those agencies under its rules is therefore also outside the scope of EU law and beyond the powers of data protection authorities or the Court of Justice of the EU.

But that would be a misreading of the legal situation. Even if the collecting of personal information by such agencies is outside the scope of EU law (or the powers of the DPAs or the CJEU), the transmission of the data to such agencies by any entities that are subject to EU data protection instruments is within the scope of EU law. Controllers of such entities and their DPOs should be aware of that and consult their DPAs whenever such contentious cases arise.

[215] See Douwe Korff *et al*, Boundaries of Law (footnote 172, above), Part 4.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

1.4.7 The "Modernised" Council of Europe Data Protection Convention of 2018

Although the 1981 Council of Europe Convention was (broadly) brought into line with the 1995 EC Data Protection Directive, by means of the addition of rules on transborder data flows and independent data protection authorities in its Additional Protocol, adopted in 2001 (as discussed at 1.3.2, above), it still, like that Directive, was getting somewhat out of date by the end of the first decade of the 21st Century. Work to "modernise" the Convention started in 2011, and the "Modernised Convention" was adopted and opened for signature on 10 October 2018.[216] At the time of writing (December 2018), it has not yet come into force: that will happen three months after five Member States of the Council of Europe will have acceded to the Modernised Convention (Art. 26(2)) – but of course even then only in respect of those Member States; in respect of other State-Parties to the 1981 Convention (and, where applicable, its Additional Protocol), the old Convention (and Protocol) will continue to apply.[217]

The Council of Europe itself has provided a very useful **overview of what is new in the Modernised Convention**, which is provided below:[218]

> The main novelties[219] of the modernised Convention can be presented as follows:
>
> **Object and purpose of the Convention (Article 1)**
>
> Under article 1 the objective of the Convention is clearly underlined, namely to guarantee to every individuals within the jurisdiction of one of the Parties (regardless of their nationality or place of residence) the protection of their personal data when undergoing processing, thus contributing to respect for their rights and fundamental freedoms, and in particular their right to privacy.
>
> Using this wording, the Convention highlights the fact that the processing of personal data may positively enable the exercise of other fundamental rights and freedoms, which can thus be facilitated by guaranteeing the right to data protection.

---

216 See: https://www.coe.int/en/web/data-protection/background-modernisation
The "Modernised Convention" was largely ready by 2014, but its formal opening for signature was delayed, partly to allow coherence with the GDPR, and partly to address concerns from one major Council of Europe Member State.
The Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS 223, is available at:
https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/223
The consolidated text of the Modernised Convention is available at:
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf –

217 By mid-December 2018, the Modernised Convention had been signed by 22 States, but not yet ratified by any. See:
https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/223/signatures?p_auth=ZmXAeCCF
The UN Special Rapporteur on the Right to Privacy has recommended world-wide ratification of the "Modernised" Convention since 2018.

218 Taken from:
https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8
Full details of all the specific textual changes in the form of a comparative chart are available at:
https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958 (26pages)

219 This [overview] presents the novelties and does not repeat the provisions which already exist since the 1981 Convention and its 2001 additional Protocol. For a complete view of the modernised Convention, please read the consolidated version published on [the Council of Europe] website. (original footnote with edits)

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Definitions and scope of application (Articles 2 and 3)

While essential notions such as the definition of personal data and the one of data subjects are not at all modified,[220] other changes are proposed in the definitions: the concept of 'file' is abandoned. 'Controller of a data file' is replaced by 'data controller', in addition to which the terms 'processor' and 'recipient' are used.

The scope of application includes both automated and non-automated processing of personal data (manual processing where the data form part of a structure which makes it possible to search by data subject according to pre-determined criteria) which falls under the jurisdiction of a party to the Convention. The omnibus nature of the Convention is preserved and the scope naturally continues to cover the processing in the private and public sectors indistinctly, as this is one of the great strengths of the Convention.

On the other hand, the Convention no longer applies to data processing carried out by a natural person for the exercise of purely personal our household activities.[221]

Furthermore, Parties are no longer provided with the possibility to make declarations aimed at exempting from the application of the Convention certain types of data processing (e.g. national security and defence purposes).

Duties of the parties (Article 4)

Each Party has to adopt in its domestic law the measures necessary to give effect to the provisions of the Convention.

Furthermore, each Party should demonstrate that such measures have actually been taken and are effective and accept that the Convention Committee may check that these requirements have been complied with. This [*new*] evaluation process of the Parties ("follow-up mechanism") is necessary to guarantee that the level of protection established by the Convention is actually afforded by the Parties.

It is important to note that international organisations now have the possibility to accede to the Convention (Article 27), as does the European Union (Article 26).

Legitimacy of data processing and quality of data (Article 5)

Article 5 clarifies the application of the principle of proportionality to underline that it should apply throughout the entire processing, and in particular in respect of the means and methods used in the processing. It is furthermore reinforced by the principle of data minimisation.

A new provision is introduced to clearly lay down the legal basis of the processing: the consent (which to be valid has to satisfy several criteria) of the data subject or some other legitimate basis laid down by law (contract, vital interest of the data subject, legal obligation of the controller, etc.).

Sensitive data (Article 6)

The catalogue of sensitive data has been extended to include genetic and biometric data (which influenced EU), as well as data processed for the information they reveal relating to trade-union membership or ethnic origin (those two latter categories are

[220] But note that extensive gloss has been added in the Explanatory Memorandum to the Modernised Convention (added footnote).

[221] Such "purely personal processing" was first excluded from data protection rules in the 1995 Data Protection Directive, in order to ensure respect for the right to private life; it is repeated in the GDPR. (added footnote).

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

being added to the existing [*in-principle*] ban on the processing of personal data revealing racial origin, political opinions or religious or other beliefs, health or sexual life and personal data relating to offences, criminal proceedings and convictions).

Data security (Article 7)

In terms of data security, the requirement to notify, without delay, any security breaches is introduced. This requirement is limited to cases which may seriously interfere with the rights and fundamental freedoms of data subjects, which should be notified, at least, to the supervisory authorities.

Transparency of processing (Article 8)

Controllers will have the obligation to guarantee transparency of the data processing and will to that end have to provide a required set of information, in particular relating to their identity and usual place of residence or establishment, on the legal basis and the purposes of the processing, the data recipients and on the categories of personal data processed. They should furthermore provide any additional information necessary to ensure a fair and transparently processing. The Controller is exempted from providing such information where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts.

Rights of the data subject (Article 9)

Data subjects are granted new rights so that they have greater control over their data in the digital age.

The modernised Convention extends the catalogue of information to be transmitted to data subjects when they exercise their right of access. Furthermore, data subjects are entitled to obtain knowledge of the reasoning underlying the data processing, the results of which are applied to her/him. This new right is particularly important in terms of profiling of individuals.[222]

It is to be associated with another novelty, namely the right not to be subject to a decision which affects the data subject, which is based solely on an automated, processing, without the data subject having her/his views taken into consideration.

Data subjects have a right to object at any time to their personal data being processed, unless the controller demonstrates compelling legitimate grounds for the processing which override their interests or rights and fundamental freedoms.

Additional obligations (Article 10)

The modernised Convention imposes broader obligations on those processing data or having data processed on their behalf.

Accountability becomes an integral part of the protective scheme, with an obligation for the controllers to be able to demonstrate compliance with the data protection rules.

Controllers should take all appropriate measures – including when the processing is outsourced – to ensure that the right to data protection is ensured (privacy by design, examination of the likely impact of the intended data processing on the rights and fundamental freedoms of data subjects ("privacy impact assessment") and privacy by default).

222 On this subject see Recommendation (2010) 13 on the Protection of Individuals with regard to Automatic Processing of Personal Data in the context of profiling and its Explanatory memorandum. (original footnote)

Exceptions and Restrictions (Article 11)

The rights laid down in the Convention are not absolute and may be limited when this is prescribed by law and constitutes a necessary measure in a democratic society on the basis of specified and limited grounds. Among those limited grounds are now included "essential objectives of public interest" as well as a reference to the right to freedom of expression.

The list of provisions of the Convention that can be restricted has been slightly extended (see references to Articles 7.1 on security and 8.1 on transparency in Article 11.1) and a new paragraph of this Article specifically deals with processing activities for national security and defence purposes, for which the "monitoring" powers of the Committee as well as some missions of the supervisory authorities can be limited. The requirement that processing activities for national security and defence purposes be subject to an independent and effective review and supervision is clearly laid down.

It is important to recall once again that contrary to the previous provisions of Convention 108, Parties to the modernised Convention will no longer be able to exclude from the scope of application of the Convention certain types of processing.

Transborder flows of personal data (Article 14)[223]

The aim of this provision is to facilitate, where applicable, the free flow of information regardless of frontiers, while ensuring an appropriate protection of individuals with regard to the processing of personal data.

In the absence of harmonised rules of protection shared by States belonging to a regional international organisation and governing data flows (see for instance the data protection framework of the European Union), data flows between Parties should thus operate freely.

Regarding transborder flows of data to a recipient that is not subject to the jurisdiction of a Party, an appropriate level of protection in the recipient State or organisation is to be guaranteed. As this cannot be presumed since the recipient is not a Party, the Convention establishes two main means to ensure that the level of data protection is indeed appropriate; either by law, or by ad hoc or approved standardised safeguards that are legally binding and enforceable (notably contractual clauses or binding corporate rules) , as well as duly implemented.

Supervisory authorities (Article 15)

Building on Article 1 of the additional protocol, the modernised Convention complements the catalogue of the authorities' powers with a provision that, in addition to their powers to intervene, investigate, engage in legal proceedings or bring to the attention of the judicial authorities violations of data protection provisions, the authorities also have a duty to raise awareness, provide information and educate all players involved (data subjects, controllers, processors etc.). It also allows the authorities to take decisions and impose sanctions. Furthermore, it is recalled that the supervisory authorities should be independent in exercising these tasks and powers.

Forms of co-operation (Article 17)

The modernised Convention also addresses the issue of co-operation (and mutual assistance) between the supervisory authorities.

223 In this respect, the Modernised Convention builds on the Additional Protocol and the EU rules.

(CC) Douwe Korff & Marie Georges/Final Text as approved – 190723

The supervisory authorities have to co-ordinate their investigations, to conduct joint actions and to provide to each other information and documentation on their law and administrative practices relating to data protection.

The information exchanged between the supervisory authorities will include personal data only where such data are essential for co-operation or where the data subject has given the specific, free and informed consent.

Finally the Convention provides a forum for increased co-operation: the supervisory authorities of the Parties have to form a network in order to organise their co-operation and to perform their duties as specified by the Convention.

Convention Committee (Articles 22, 23 and 24)

The Convention Committee plays a crucial role in interpreting the Convention, encouraging the exchange of information between the Parties and developing data protection standards.

The role and powers of this Committee is strengthened with the Modernised Convention. It no longer is limited to a "consultative" role but also has assessment and monitoring powers. [*Apart from providing*] opinion[*s*] on the level of data protection provided by a state [*as before, it will now also do so in respect of*]international organisation[*s*] before accession to the Convention. The committee is also [*now*]able to assess the compliance of the domestic law of the Party concerned and determine the effectiveness of the measures taken (existence of a supervisory authority, responsibilities, existence of effective legal remedies).

It is also able to assess whether the legal norms governing the data transfers provide sufficient guarantee of an appropriate level of data protection.

This is not the place to analyse these novelties in detail. Suffice it to note that **they bring the new, "modernised" Convention regime close to the new regime established for the EU under the GDPR**. This means that when the EU will assess the "adequacy" of a data protection regime in a third country (as discussed in Part Two, section 2.1), the fact that that third country is a party to the Modernised Convention would be a major matter to be taken into account.

Indeed, in terms of **scope**, the Modernised Convention exceeds the GDPR, in that, as is made very clear both in the text of the Modernised Convention and in the above overview, State-Parties to the Modernised Convention will **no longer be able to exclude** any types of processing from their obligations – such as ***national security*** and ***defence***, which are matters outside the scope of the EU data protection instruments.[224]

Whether in other respects the Modernised Convention – or to be more precise, the national laws of the State-Parties to the Modernised Convention that implement that Convention – will always be fully in line with the GDPR – or to be more precise, with the GDPR as it will in future be interpreted and applied by the EU's new European Data Protection Board, the EU

[224] See section 1.3.1, above, under the heading "*Nature and limitations of EC directives*", as concerns this limitation in relation to the 1995 and 2002 EC data protection directives, and Part Two, section 2.1, below, as concerns the GDPR. In relation to processing for law enforcement (etc.) purposes, and processing by the EU institutions themselves, the EU of course does have rules in place, which essentially conform to the GDPR (and thus the Modernised Convention) standards (or in relation to the EU institutions, will do so once these have been brought into line with the GDPR).

Member States' data protection authorities, the European Commission and the CJEU – is of course a matter that remains to be seen.

For instance, the new rules on transborder data flows in the Modernised Convention allow transfers to third countries that provide an "***appropriate"***level of protection (Art. 14) – which on the face of may look similar to the requirement of an "***adequate***" level of protection in the GDPR (as under the 1995 Data Protection Directive) – but it remains to be seen whetheror how the new Convention Committee will follow the CJEU in holding that the term "appropriate" should be interpreted as meaning that the third country in question must provide "***essentially equivalent***" protection (as the CJEU ruled in interpreting the term "adequate").[225]

In other respects, e.g., as concerns **consent by children**, the Modernised Convention is not as detailed or specific as the GDPR.

But those matters aside, it is clear that between them, the Council of Europe and the European Union are leading the way in setting the global "gold standards" for data protection, both as applicable within states and as concerns transnational data flows.

Finally, it should be noted that the Modernised Convention (unlike its predecessor) is open for accession by international organisations – and the EU can therefore also formally sign up to it.

- o – O – o -

[225] CJEU, *Schrems* judgment, (footnote 73, above), para. 73. CJEU judgment in Case C-362/14, 6 December 2015

PART TWO

The General Data Protection Regulation

2.1 Introduction

As already noted at 1.4.1, above, the General Data Protection Regulation (GDPR or "the Regulation") was adopted, partly because the 1995 Data Protection Directive had not led to a sufficient level of harmonisation of the laws in the Member States; partly in response to the massive expansion in the processing of personal data since the introduction of the 1995 Data Protection Directive; and partly in response to the case-law of the CJEU. It remains to be seen if it will suffice to fully address the development of ever-more-intrusive technologies, such as Big Data, the Internet of Things, algorithmic decision-making and the use of artificial intelligence.

The Regulation builds on the 1995 Data Protection Directive but significantly expands on it and, in doing so, considerably strengthens the main EU data protection regime. It brings*greater harmonisation*, *stronger data subject rights*, *closer cooperation between data protection authorities*,*stronger enforcement powers* – and more.

Attachment 1 to this handbook provides an *Index of the chapters, sections and articles of the GDPR*, for easy reference. Attachment 2 provides the full text of the Regulation as published in the Official Journal of the EU, including the recitals.

Section 3.2 explains the status and approach of the GDPR, and discusses in some detail the implications of the fact that it contains many clauses allowing for further regulation at the national level (thus somewhat undermining the aim of fuller harmonisation).

Section3.3provides a chapter-by-chapter, section-by-section and article-by-article overview of the GDPR.

We then turn to the two core issues for DPOs: the new "accountability" (duty to demonstrate compliance) principle (section 3.4) and the rules on the appointment, requirements, conditions and tasks (etc.) of the DPO (section 3.5), and explain the link between those two.

2.2 Status and approach of the GDPR: direct applicability with "specification clauses"

A regulation …

The GDPR is a **regulation** – that is: an EU law that is ***directly applicable*** in the legal orders of the EU Member States (and the non-EU EEA states), without having to be "transposed" into national law, as is the case with directives such as the 1995 Data Protection Directive.

The EU legislator chose this route precisely because implementation of the 1995 directive had been uneven: it was differently implemented in different Member States, leading to a lack of harmonisation.[226]

[226] This was already the conclusion reached in an EU-commissioned study by Douwe Korff for the University of Essex, Report on an EU study on the implementation of the [1995] data protection directive, 2002, available at:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667 –
but it took the EU another 10 years to address this by proposing a regulation.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Moreover, it was deficiently implemented in at least some of them, such as the UK.[227]

In theory, a regulation, being directly applicable, should lead to **full harmonisation** of the law in the area it covers. In the case of the GDPR, this is reinforced by much stronger arrangements for**information sharing and cooperation** between the regulators (the national supervisory- or data protection authorities, DPAs) and a special **"consistency" mechanism**, as discussed below, under that heading.

However, as shown under the next sub-heading, at the same time the GDPR still leaves many issues to be further regulated in the national laws of the EU Member States, according to their internal legal or institutional system. This could, in some areas, undermine the aim of full harmonisation, but as we shall discuss under the headings "*Requirements of "specificationclauses*" and"*Cooperation and consistency*", there are also limits to the freedom of Member States in this respect, and new means of EU-level oversight, also of the exercise of these "flexibilities" (at least in theory).

… but with "specification clauses"[228]

Although the Regulation aims at greater harmonisation, it still contains numerous "flexible" provisions, referred to by the Commission as "specification clauses", that defer to law in the Member States, in particular in relation to the public sector, but also in relation to duties imposed by national law on companies subject to the relevant Member State's jurisdiction (e.g., under employment law, or law enforcement rules) and on the composition of a DPA.

Types of "specification clauses"

The Italian data protection authority, the *Garante della Privacy*, has identified four different (although somewhat overlapping) types of clauses that leave room for further regulation by Member State law:[229]

- **Further specifications**

  These are provisions under which a Member States may maintain or introduce "*more specific provisions to adapt the application*" of the relevant provision in the Regulation (various phrases to this effect are used).

  Examples:

  Member States may specify what processing operations require ***prior authorisation***, or regulate the use of ***national identity numbers***, or the processing of ***personal data on employees***.

  Member States may "*maintain or introduce **further conditions, including limitations**, with regard to the processing of **genetic data**, **biometric data** or **data concerning***

---

[227] According to the EU Commission, in 2011, almost a third of the 34 articles in the Directive had by that time not been implemented properly by the UK, see: http://amberhawk.typepad.com/amberhawk/2011/02/european-commission-explains-why-uks-data-protection-act-is-deficient.html
Although the Commission threatened to take enforcement action, it did not actually pursue this even though the deficiencies were never properly or fully remedied.

[228] See the sub-section on "*Relationship between the e-Privacy Directive and the GDPR*", above.

[229] Antonio Caselli, *Garante* staff member, presentation to the first "T4DATA" training session, June 2018, on "*GDPR and national rules*". The substance of this presentation is written up and expanded upon in some detail in Attachment 4 to the handbook (in Volume Two), where further examples are also given.

health", over and above the conditions and limitations imposed by the GDPR itself in Article 9(1) – (3) (the article dealing with "special categories of personal data", usually referred to as "sensitive data") (Art. 9(4)). They may thus, for instance, stipulate that ***prior consent*** is always required for the processing of **genetic data**.

- **Options and choices**

In some respects, the GDPR allows Member States, through their national law, to **choose** from certain options specifically set out in the Regulation, or to extend an obligation or prohibition that under the GDPR applies only in certain cases, to other cases.

For example, Member States may allow ***children*** aged over 13, 14 or 15 to ***consent to certain information services***, rather than only from the age of 16 as set out in the GDRP; or may require ***the appointment of a DPO*** where the GDPR does not do so.

- **Restrictions and derogations**

Subject to certain rather broadly-phrased **conditions** (discussed below, under the headings "*Requirements of 'specification clauses'*" and "*Problems posed by 'specificationclauses'*"), Article 23 GDPR allows for **sweeping restrictions** on essentially all data subject rights in relation to broadly defined **important objectives of public interest**: ***national security***, ***defence***, ***public security***, ***law enforcement*** and ***judicial independence*** – but also ***protectingthe economic or financial interests of the state***, enforcement of ***professional ethics***, any kind of "***monitoring, inspection or regulatory function*** connected, even occasionally, to the exercise of official authority" in any of the main protected interest, "the ***protection of the data subject or the rights and freedoms of others***" and the ***enforcement of civil claims***.

Articles 85, 86 and 89 GDPR all contain provisions that, on the one hand, allow for (and in some respects, require) **derogations** from certain rules in the GDPR in order to protect **freedom of expression**, allow **freedom of information** (access to documents and information held by public authorities) and **archiving**, and facilitate (publicly beneficial) **research**, while on the other hand imposing certain **conditions** on those derogations (as also further discussed under the headings "*Requirements of 'specification clauses'*" and "*Problems posed by 'specification clauses'*", below).

Note: Some of these special rules serve to protect the interests of "others", while others can be seen as being in the general or public interest, and some, like freedom of information, can serve both. These are matters in which the rules have up to now not been harmonised, although in some EU Member States supervision over both data protection and freedom of information has been put in the hands of the same authorities. Given that such matters are increasingly transnational – e.g., cross-border requests for access to public data; freedom of expression vs. data protection and privacy issues relating to online publications; and transnational medical research – it is to be expected that the EDPB will issue further guidance on these matters, in particular in relation to such transnational activities. The Commission could also propose new initiatives in these areas.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

- **Regulatory duties**

  In some respects other than those noted above – in particular, in relation to the establishment of independent supervisory bodies (data protection authorities, DPAs), and the establishment of certification schemes – the GDPR **requires** the Member States to adopt detailed rules and regulations, implementing the relevant requirements for DPAs in their national legal order. These are largely technical issues (although they also require compliance with important standards, e.g., on independence and the provision of sufficient resources).

Requirements of "specification clauses"

In many respects, including those mentioned under the headings "*further specifications*" and "*options and choices*", above, but most especially those noted under the heading "*restrictions and derogations*", the GDPR **requires** Member States to adopt **legal rules** to address the relevant matters ***that meet certain democratic/human rights standards***.

Other provisions (not included under those headings) also **imply the need for regulation**, in that they require Member States to adopt "***appropriate safeguards***", "***suitable safeguards***"or "***adequate measures***". Since the GDPR itself often does not clarify what those safeguards or measures might be, the Member States will have to clarify this in the national laws – which again will have to meet certain democratic/rule of law***standards***.

It is important to note that **in this, Member States are not simply given unfettered discretion** – as is clear from requirements that certain measures or safeguards be "appropriate" or "suitable". In other respects, certain generally applicable **rule of law-standards** and -conditions are expressly spelled out in the GDPR – but in fact, similar standards and conditions apply to all relevant regulation.

Thus, the GDPR expressly stipulates that the in principle sweeping derogations allowed under Article 23 (summarised above under the heading "*Restrictions and derogations*") must be set out in **law** (a "***legislative measure***") which must "***respect[] the essence of the fundamental rights and freedoms*** *and [be] a* ***necessary and proportionate*** *measure in a democratic society to safeguard*" the relevant interest. These requirements are direct reflections of the requirements that must be met by any limitation on any of the main rights protected by the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights (CFR). To quote the latter:

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and **respect the essence** of those rights and freedoms. Subject to the principle of **proportionality**, limitations may be made only if they are **necessary** and **genuinely meet objectives of general interest** recognised by the Union or **the need to protect the rights and freedoms of others**.
>
> (Art. 52(1), emphases added)

Since any Member State law limiting or restricting any data subject rights under any of the "specification clauses" in the GDPR must be seen as inherently constituting a limitation of the right to data protection as guaranteed in the CFR (Article 8), they must all meet the above standards.

More specifically, under the ECHR and the CFR, and thus also under the GDPR, the relevant law must meet certain crucial **"quality" requirements**: the rules in the law must be

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

"**compatible with the rule of law**" (which means in particular that they may not be ***discriminatory*** or ***arbitrary***, and must be ***challengeable*** and subject to ***effective remedies***) and, morein particular, **accessible** (i.e., ***published***) andsufficiently **clear** and **precise** to be "***foreseeable***" in its (and their) application.[230]

The reference to "respect [for] the **essence**" of the rights and freedoms in question must be read as **prohibiting any legal rule that so deeply impinges on a right as to render it nugatory**. For instance, the Court of Justice of the EU has held that:[231]

> legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter…

Member States derogations under Article 23 GDPR in particular – including derogations from data protection rules in order to safeguard national security and defence – may therefore never amount to such never-warranted and never-acceptable excessive derogations from the main rules.

More specifically, any derogations under Article 23, and indeed any other departures from any of the normal rules in the GDPR under any of the "specificationclauses", must meet the "**necessary and proportionate in a democratic society**" test. This means that any departure from the normal rules or restriction of any non-absolute data subject right, based on a "specification clause", must genuinely be in pursuit of the claimed "***legitimate aim***"/"***important objective of public interest***", respond to a "***pressing social need***", and be "***reasonably proportionate***" to that need. In judging what exactly is needed in those terms, States may be granted a certain "***margin of appreciation***"[232] – but this margin is limited by the requirement that the measure (the derogation or limitation) must be necessary "***in a democratic society***".

Broadly speaking, if there is **clear guidance** on a particular matter – such as has been provided under the 1995 Data Protection Directive by the Article 29 Working Party and the EDPS, and is now being provided under the GDPR by the European Data Protection Board (which includes the EDPS) – and/or if there is a **notable convergence of views** on the matter between the Member States (or the Member States' DPAs), then any divergence from such guidance or consensus by one Member State is likely to indicate that the divergent measures (derogations or limitations that go beyond what is deemed necessary or

---

230 See: Harris, O'Boyle &Warbrick, Law of the European Convention on Human Rights, 2nd ed., 2009, Chapter 8, section 3, *Limitations*. For a simple overview of the relevant ECHR requirements, see: Douwe Korff, The standard approach under articles 8 – 11 ECHR and article 2 ECHR (teaching handout), available at: https://www.pravo.unizg.hr/_download/repository/KORFF_-_STANDARD_APPROACH_ARTS_8-11_ART2.pdf See in particular the text under questions 3 (Law) and 5 (Necessary and proportionate) in that handout.

231 CJEU, *Schrems* judgment, (footnote 73, above), para. 94.

232 The "margin of appreciation" doctrine, which is strongly embedded in the case-law of the European Court of Human Rights, is less clearly enunciated by the Court of Justice of the EU which, if anything, tends to refer to the "discretion" or "margin of discretion" accorded to Member States in certain matters. But for the purposes of the present handbook, the doctrine may be regarded as reflected in the case-law of both the Strasbourg and the Luxembourg courts, even if perhaps to somewhat different degrees and somewhat dependent on context. See: Francisco Javier Mena Parras, From Strasbourg to Luxembourg? Transposing the margin of appreciation concept into EU law, Brussels, 2008, available at: http://www.philodroit.be/IMG/pdf/fm_transposing_the_margin_of_appreciation_concept_into_eu_law_-_2015-7.pdf

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

proportionate in other Member States) are not "necessary" or "proportionate" "in a democratic society".

However, as noted under the next heading, these matters cannot be resolved by means of the "cooperation- and consistency mechanisms" (discussed separately, later).

Problems posed by "specification clauses"

We have dwelled on the "specification clauses" in some detail because they pose problems in the effective application of the GDPR. Those come in two forms.

First of all,"specification clauses" will by their very nature lead to **different (or more or less detailed) rules, reflecting national idiosyncrasies, on identical issues in the different Member States**. This does not pose so much of a problem in relation to processing that takes place entirely within one Member State, and that relates only to data subjects in that Member State. However, as noted earlier, in the 21st Century, more and more state activities have international implications and involve cross-border personal data processing operations, also in the public sector, and not only in relation to law enforcement or borders. This is especially the case within the EU, because of the "four freedoms" that are fundamental to the European project: the freedom of movement for goods, services, people and finance.

When goods or services are offered and purchased across border, within the EU as without, personal data follows (and is essential for) the transactions. When people move, so does their data: their data on tax, welfare and pension benefits, their medical data, marriage, births, divorce, death and residence records. When payments are made (between individuals, or between individuals and private entities, or between individuals and state agencies, be that the tax-,residency- or pension office), this entails flows of their financial and other data. This is the case *a fortiori* when the processing, or some of the processing, takes place online.

When, in such circumstances, there are different rules in the different Member States concerned on the processing of the data in question, this gives rise to potential (and potentially serious) **legal issues** that will have to be resolved on a case-by-case basis (which will often not be easy). The following examples may illustrate this with reference to some of the specific derogations and limitations that may be introduced under the "specification clauses" mentioned earlier:

Examples:

- If one MS imposes restrictions on the use of the national identity number that are not imposed in another MS, are those restrictions still to be adhered to by a recipient in the latter MS (including a public sector recipient) if the number is transferred to that recipient?
- If one MS imposes "further conditions" or additional "limitations" on the processing of all or certain types of sensitive data (e.g., on the use of biometric or genetic data) that are not imposed in another MS, are those conditions or limitations still to be adhered to by a recipient in the latter MS (including a public sector recipient) if the data are transferred to that recipient?
- If one MS sets the age of consent to the use of information services for children at the age of, say, 14, and another MS leaves it at the GDPR-proposed age of 16, may

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

an information service provider in the former MS provide its service to a child aged 14 in the latter MS, on the basis of the 14-year old's consent? Should the provider distinguish on the basis of the IP-address of the child (even though that can be easily "spoofed" by means of a VPN, even by 14-year olds)?

- If one MS requires the obtaining of prior authorisation from the DPA for processing in relation to social protection and public health, but another MS does not, may a public authority in the latter MS process personal data in relation to data subjects in the former MS for such purposes, without such prior authorisation – as could easily happen in relation to children of migrants who leave their spouse and children in their home country while working in another MS, but with child benefit etc. being paid to the spouses in the home country? (NB: In the context of providing such prior authorisation, the relevant DPA will presumably impose or require the imposition of certain safeguards and restrictions. Must the state agency in the other MS comply with those too? Would the agency even be aware of them?)

The above issues are seriously aggravated by **the absence from the GDPR of an "applicable law" provision** on the lines of the one contained in the 1995 Data Protection Directive (even if that provision, Article 4,raised questionsin relation todifferentlanguage translation and in terms of effectiveness.[233]. Presumably, such a provision was left out of the GDPR because it was assumed that, as a regulation, it would be applied in a fully-harmonised way – but as shown above, in the (many) areas covered by "specification clauses" (to be dealt with at the national level in specific laws) this is manifestly not going to be the case.

The second issue relates to **compliance with the rule of law-requirements** set out above, under the previous sub-heading. Questions are likely to arise about whether certain laws in certain Member States that restrict certain rights or relax certain rules meet those test, i.e., whether they are sufficiently accessible, precise and foreseeable in their application, necessary or proportionate to the relevant (legitimate/important) aim.

Those issues can often not be resolved, or even addressed, under the "cooperation- and consistency mechanisms" discussed later, because those mechanisms are limited to cooperation in relation to measures taken or proposed to be taken by the data protection authorities: they cannot be used to remedy deficiencies in the laws of the Member States. This can create serious problems, especially in relation to transfers of personal data from a state agency in one EU Member State to a state agency in another Member States, if in the latter state the data will be processed under laws that arguably do not meet the rule of law-requirements. Still, experience in other areas (such as the Justice and Home Affairs rules, not discussed in this first edition of the handbook) shows that where necessary, action to address such issues can be taken, especially on the basis of Commission or EDPB suggestions or proposals.

Implications for DPOs

It should be clear from the above that DPOs should be aware of, and **study, not just the rules in the GDPR but also any relevant domestic rules that build on "specificationclauses" in the GDPR** – and to some extent indeed the relevant laws and rules in other Member

[233] See Douwe Korff, *The question of "applicable law"*, in: Compliance Guide 3 – Interim report, Privacy Laws & Business, November 1999.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

States and in third countries, if their organisation discloses personal data to such other states.

These can take many forms. In some cases, Member States may simply have retained rules that were in place already before the GDPR came into force, including special derogations to protect important public interests, or to facilitate research – although **those may not always meet the rule of law requirements of the relevant "specification clause" or be "appropriate" or "suitable" in terms of the GDPR** (as discussed above). In other cases, their Member State may have adopted specific laws or legal rules to "further regulate" matters left to the Member State under the GDPR, or to clarify which options are used, etc. In yet other cases, the Member State may as yet not have clarified the national application of the relevant clauses at all.

DPOs can of course not themselves rectify any deficiencies or issues in these respects. However, within their own networks of DPOs, and in their interactions with their national data protection authorities,[234] they can **flag up such issues and encourage appropriate action**. They should also – again, preferably, together with other DPOs working in similar organisations – **alert the higher echelons of their own organisations** (in the public sector, for instance, the relevant government minister(s)) to such perceived deficiencies.In such situations DPOs have to develop strategically efficient approaches.

2.3 Overview of the GDPR

Below follows a broad, chapter-by-chapter and section-by-section overview of the GDPR.*

* It is hoped that for a future, expanded second edition of this Handbook a short article-by-article commentaryon all the GDPR provisions can be produced, which will focus on the concrete, practical application of the relevant provisions. In the meantime, DPOs are advised to consult one of the main academic commentaries that are being published in several languages, as well, of course, as the official guidance issued by national DPAs, the EDPB and national and European courts.

2018 GENERAL DATA PROTECTION REGULATION:
Chapter I: **General provisions (Article 1 – 4):** - Subject matter and objectives of the Regulation; - Material scope; - Territorial scope; - Definitions.
Chapter II: **Principles (Articles 5 – 11):** - Principles relating to processing of personal data; - Lawfulness of processing [legal bases]; - Conditions of consent; - Conditions applicable to child's consent in relation to information society services; - Processing of special categories of personal data [sensitive data]; - Processing of personal data relating to criminal convictions and offences; - Processing which does not require identification.

[234] Cf. the **French** DPO "Extranet" that could be useful in such contexts. See footnote 456, below.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Chapter III:

Rights of the data subject

Section 1 (Article 12):

Transparency and modalities:

- Transparent information, communication and modalities for the exercise of the rights of the data subject.

Section 2 (Articles 13 – 15):

Information and access to personal data:

- Information to be provided where personal data are collected from the data subject;
- Information to be provided where personal data have not been obtained from the data subject;
- Right of access by the data subject.

Section 3 (Articles 16 – 20):

Rectification and erasure:

- Right to rectification
- Right to erasure (Right to restriction of processing 'right to be forgotten')
- Right to restriction of processing ["blocking"]
- Notification obligation regarding rectification or erasure of personal data or restriction of processing
- Right to data portability

Section 4 (Articles 21 – 22):

Right to object and automated individual decision-making:

- Right to object;
- Automated individual decision-making, including profiling.

Section 5 (Article 23):

Restrictions

CHAPTER IV:

Controller and processor

Section 1 (Articles 24 – 31):

General obligations:

- Responsibility of the controller;
- Data protection by design and by default;
- Joint controllers;
- Representatives of controllers or processors not established in the Union;
- Processor;
- Processing under the authority of the controller or processor;
- Records of processing activities;
- Cooperation with the supervisory authority.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Section 2 (Articles 32 – 34):

Security of personal data:

- Security of processing;
- Notification of a personal data breach to the supervisory authority;
- Communication of a personal data breach to the data subject.

Section 3 (Articles 35 – 36):

Data protection impact assessment and prior consultation:

- Data protection impact assessment;
- Prior consultation.

Section 4 (Articles 37 – 39):

Data protection officer:

- Designation of the data protection officer;
- Position of the data protection officer;
- Tasks of the data protection officer.

Section 5 (Articles 40 – 43):

Codes of conduct and certification:

- Codes of conduct;
- Monitoring of approved codes of conduct;
- Certification;
- Certification bodies.

CHAPTER V (Articles 44 – 50):

Transfers of personal data to third countries or international organisations:

- General principle for transfers;
- Transfers on the basis of an adequacy decision;
- Transfers subject to appropriate safeguards;
- Binding corporate rules;
- Transfers or disclosures not authorised by Union law;
- Derogations for specific situations;
- International cooperation for the protection of personal data.

CHAPTER VI:

Independent supervisory authorities:

Section 1 (Articles 51 – 54):

Independent status:

- Supervisory authority;
- Independence;
- General conditions for the members of the supervisory authority;
- Rules on the establishment of the supervisory authority.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Section 2 (Articles 55 – 59):

Competence, tasks and powers:

- Competence;
- Competence of the lead supervisory authority;
- Tasks;
- Powers;
- Activity reports.

CHAPTER VII:

Cooperation and consistency

Section 1 (Articles 60 – 62):

Cooperation:

- Cooperation between the lead supervisory authority and the other supervisory authorities concerned;
- Mutual assistance;
- Joint operations of supervisory authorities.

Section 2 (Articles 63 – 67):

Consistency:

- Consistency mechanism;
- Opinion of the Board;
- Dispute resolution by the Board;
- Urgency procedure;
- Exchange of information.

Section 3 (Articles 68 – 76):

European data protection board:

- European Data Protection Board;
- Independence;
- Tasks of the Board;
- Reports;
- Procedure;
- Chair;
- Tasks of the Chair;
- Secretariat;
- Confidentiality.

CHAPTER VIII (Articles 77 – 84):

Remedies, liability and penalties:

- Right to lodge a complaint with a supervisory authority;
- Right to an effective judicial remedy against a supervisory authority;
- Right to an effective judicial remedy against a controller or processor;
- Representation of data subjects;
- Suspension of proceedings;
- Right to compensation and liability;
- General conditions for imposing administrative fines;
- Penalties.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

CHAPTER IX (Articles 85 – 91): **Provisions relating to specific processing situations:** - Processing and freedom of expression and information; - Processing and public access to official documents; - Processing of the national identification number; - Processing in the context of employment; - Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; - Obligations of secrecy; - Existing data protection rules of churches and religious associations.
CHAPTER X (Articles 92 – 93): **Delegated acts and implementing acts:** - Exercise of the delegation; - Committee procedure.
CHAPTER XI (Articles 94 – 99): **Final provisions:** - Repeal of Directive 95/46/EC; - Relationship with Directive 2002/58/EC; - Relationship with previously concluded Agreements; - Commission reports; - Review of other Union legal acts on data protection; - Entry into force and application.

2.4 The accountability principle[235]

2.4.1 The new duty to be able to demonstrate compliance

Although this may appear to be nothing new (and can be said to be inspired by the American legal approach, which was in turn reflected in the OECD Guidelines of 1980), it is actual one of the main features of the new EU General Data Protection Regulation (GDPR) – perhaps even *the* main feature – that it lays great emphasis on the fact that:

> **The controller shall be responsible for, *and [shall] be able to demonstrate compliance with*, [the principles relating to processing of personal data] ('accountability')"** (Art. 5(2)).

As the Italian data protection authority, the *GarantedellaPrivacy*, puts it:[236]

> To make an entity *accountable* means to assign actions and decisions to that entity **and to expect that entity to be answerable for those actions and decisions**. Therefore, accountability is **the state of being answerable** for the actions and decisions that have been assigned.

[235] This section draws on, and in parts repeats or summarises, Douwe Korff, The Practical Implications of the new EU General Data Protection Regulation for EU- and non-EU Companies, August 2016, paper presented at CMS Cameron McKenna LLP, London, in February 2017, available at: http://ssrn.com/abstract=3165515

[236] Luigi Carrozzi, presentation to the first "T4DATA" training session, June 2018, slide on "*Asset inventory and the Accountability Principle*" (original emphases).

The novelty lies not in the body in charge of the processing being responsible for compliance – that was of course also already the case under the 1995 Data Protection Directive (although that directive does not use the term "accountability"). Rather, the novelty is the emphasis on the controller (and in some cases the processor) being required to "**demonstrate**" this compliance: the Regulation uses the term no less than 33 times.

This contrasts with the 1995 Directive, which nowhere explicitly required a controller or processor to demonstrate compliance with anything (unless of course they were required to do so by a DPA or a court). More specifically, the various "notification" or "registration" schemes established under the Directive inat least some countries did little to demonstrate such compliance,[237] while in others they were only successful by being very detailed and presented in such a way as to nudge the controllers towards applying all the legal requirements to any new data processing operation, with the relevant data protection authority (DPA) alerting the controller and suggesting modifications or giving advice when necessary or required. In the context of rapidly expanding and evolving data processing practices, and in countries (such as the EU Member States) where there is already some significant knowledge of and experience with the application of data protection rules and principles, also in a context of the promotion of "social responsibility" of organisations, a new approach emphasising the primary responsibility and accountability of those processing personal data (be that as controller or processor) was called for. That is what the accountability principle and the duty to demonstrate stand for.

As discussed in section 2.3, below, the Regulation requires the appointment of Data Protection Officers (DPOs) for all public- and many private-sector controllers as the main institutional means to put the accountability principle into practice.

As the stipulation of the accountability principle in Art. 5(2), quoted above, makes clear, the duty to demonstrate compliance applies first of all to the basic principles underpinning the Regulation, set out in Art. 5(1), i.e., tolawfulness, fairness and transparency; narrow and explicit purpose specification and purpose limitation; data minimisation (including adequacy, relevance and necessity of data); accuracy(including up-to-dateness); storage (retention) limitation; integrity,confidentiality and security. Of course, it also applies (if anything *a fortiori*) to the especially strict application of these principles to processing involving special categories of data (so-called sensitive data – Art. 9) or that are otherwise likely to result in a high risk to the rights and freedoms of natural persons (and which therefore require a special Data Protection Impact Assessment – Art. 35).

Beyond this, the Regulationexpressly or implicitly imposes a duty to demonstrate compliance in many more specific contexts, including in relation to:

- The obtaining of consent (when required) (see Art. 7(1));
- Refusal of a request by a data subject for accessto or rectification of data (see Arts. 11(2) and 12(5));
- Non-compliance with data subjects' objections to processing (see Art. 21(1));
- The provision of "sufficient guarantees" of competence and the taking of "appropriate technicaland organisational measures" to ensure security of data processing,by processors and sub-processors (see Arts. 28 and 32);

[237] See GDPR, Recital 89.

- The provision of "appropriate safeguards" for transfers of personal data to third countries without adequate data protection (Art. 46);
- Etcetera.

Closely related to this duty of compliance demonstrability are the new general and specific duties the GDPR imposes in terms of:

- **creating a register of personal data processing operations**;
- carrying out of a **general review of those operations**;
- **assessing the risks** to the rights and freedoms of individuals posed by those operations;
- performing in-depth **data protection impact assessments**in relation to operations that are assessed aslikely to result in a "***high risk***";
- using**data protection by design and default**in relation to all personal data processing operations;
- **data breach notification** requirements.

We will look at all of these, and in particular at the role of DPOs in relation to them, in some detail in Part Three. Here, brief mentions and cross-references to that part can therefore suffice.

Thus, first of all, the Regulation imposes a crucial **general requirement to keep detailed recordsof all of the controller's personal data processing operations**, setting out the specific details of each and every operation (Art. 30); these records should be held in a **register of personal data processing operations** and must demonstrate that, and how, both the above general duties and any more specific ones are complied with (cf. Recital 82). See the discussion of Task 1 in Part Three of this handbook.

Secondly, the Regulation requires controllers, with the help of their DPOs, to **review their operations** and where necessary bring them into line with the Regulation, and to note the review and any remedial action taken in the above-mentioned register. See the discussion of Task 2 in Part Three of this handbook.

Third, the Regulation imposes a general duty on controllers to "take into account" the **risks** posed by the controller's proposed processing operation, **coupled with** a duty to implement "***appropriate technical and organisational measures***" to counter those risks and a duty "*to demonstrate that processing is performed in accordance with this Regulation*" – i.e., the Regulation requires that those risks have indeed been assessed and that the measures taken in the light of that assessment were appropriate to those risks (Art. 24(1); cf. also Art. 32). These matters too should be duly recorded. See the discussion of Task 3 in Part Three of this handbook.

Fourth, if the general risk assessment (noted above) shows that there is a likelihood of a**high risk** to the rights and freedoms of natural persons, the controller must, prior to the processing, carry out a **data protection impact assessment (DPIA)** of the envisaged processing operations on the protection of personal data, and document this assessment. The DPIA document must contain: a systematic description of the envisaged processing operations and the purposes of the processing; an assessment of the necessity and proportionality of the processing operations and of the data in relation to those purposes;

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

an assessment of the risks to the rights and freedoms of data subjects posed by the processing; and a description of the measures envisaged to address those risks, including "*safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned*" (Art. 35). See the discussion of Task 4 in Part Three of this handbook.

Fifth, the Regulation imposes a general duty on controllers to use "**Data Protection-by-Design and -Default**", in both the setting up and the carrying out of all of the controller's processing operations (Art. 25) – and the controller must be able to demonstrate that this has been done. In this respect, the Regulation mentions that certifications (data protection seals) can be used as an "element" to demonstrate compliance (Art. 25(3), further discussed below). See the discussion of Task 9 in Part Three of this handbook.

And sixth, controllers must **document full details of all personal data breaches** (personal data security breaches) and remedial actions taken, and **notify** the relevant (competent) supervisory authority of those details within 72 hours (Art. 33). The data subjects affected by the breach must also be informed, but only if "the personal data breach is likely to result in a high risk to [their] rights and freedoms", and in less specific detail (Art. 34). See the discussion of Task 6 in Part Three of this handbook.

The Regulation also contains some more specific recording duties, including the stipulation that if two or more controllers jointly determine the purposes and means of processing, they are joint controllers. As such, they must "in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation" in the form of "**an arrangement between them**"; and this "arrangement" "shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects". In practice, since the controllers may be asked by the supervisory authorities to show compliance with these duties, the arrangement will have to be **in writing or in a comparably reliable electronic format** (Art. 26).

And of course the various stipulations in the Regulation requiring controllers, joint controllers, processors and sub-processors to specify the arrangements between them and/or in relation to data transfers in **contracts or similar legally binding instruments** also require documentation.

2.4.2 Means of demonstrating compliance

The general duty to keep detailed **registers and records**, and the more specific record-keeping duties imposed in relation to joint controllers, data breaches and DPIAs, mentioned above, constitute the main, general means of demonstrating compliance, provided for in the Regulation.

Those records should reflect a general data protection-promoting culture and approach, reflected in such **practices** as:

- drawing up and formally adopting internal data protection policies (and taking associated action, such as training);
- incorporating data protection by design- and data protection by default principles in all of the controller's data processing operations, products and services, at each step, from their conception through to their actual operation;

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

- minimising the use and retention of personal data, and more specifically the use of still-identifiable data (using pseudonymisation or anonymisation of previously identifiable data whenever possible);
- ensuring the fullest transparency about the controller's operations to data subjects and the general public, in paper forms, web forms and in clear and much more differentiated data protection/privacy statements on websites (e.g., clearly distinguishing,directly on the page from which personal data are collected, between mandatory and optional fields/purposes and data, and allowing for much greater legitimate choice by websiteusers, by clicking on a box), and by putting in place effective and efficient means to deal with data subject requests for general or specific information; and
- ensuring that the controller her- or himself can continue to effectively monitor the operations, in particular as concerns security (by means of access and alteration logs, etc.; and is able to enhance security whenever necessary (e.g., by issuing "patches").

(Cf. Recital 78)

In Part 3, we will look at all these matters further and in greater detail, with specific examples and practical guidance on how to perform the above tasks.

But in addition, the previous recital (77) lists various **special means** of demonstrating compliance, i.e.:

- acting in accordance with an approved code of conduct;
- acting in accordance with an approved data protection certifications;
- acting in accordance with guidelines provided by the European Data Protection Board;

and of course:

- acting in accordance with an indications provided by a data protection officer.

To these can be added, in particular in relation to cross-border transfers and sharing of personal data:

- Binding Corporate Rules (BCRs);
- administrative agreements ("arrangements") between public authorities or bodies; and
- standard- or individually-approved data transfer contracts.

In relation to data breaches, notification (and the details set out in the notification) can also be seen as a special means of demonstrating compliance with the relevant requirements.

However, it should be stressed that in relation to all of these, while they may constitute "elements" in an overall effort to demonstrate compliance, and "special means" to do so, they do not necessarily constitute legal proof ofcompliance.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

2.4.3 Evidentiary value of the various means of demonstrating compliance

In most regards, adherence to any of the above means of compliance "an element by which to demonstrate compliance", i.e., they create a presumption of compliance, but that presumption is rebuttable. If a data protection authority were to investigate a matter further, it could find that, irrespective of formal adherence to such guidelines, codes, certifications, agreements, contracts or rules, in the specific case the Regulation was nevertheless not complied with (although any good-faith effort of compliance would of course have a significant impact on the level of any penalty, if indeed any were imposed – cf. Art. 83).

2.5 The Data Protection Officer (DPO)

2.5.1 Background

The concept of public- and private sector controller-appointed data protection officers comes from German data protection law, which has long required them.[238]Even in countries that underthe 1995 Data Protection Directive have not required the appointment of DPOs by law (such as Austria, which in other respects often follows the German example), or only included as an option (as in France), the institution has often become widely adopted. In several countries, there are national associations of DPOs, and there is also a Confederation of European Data Protection Organisations, CEDPO,which has issued "practical guidelines for organisations" on "choosing the best candidate" as DPO.[239]At the global level, there is the USA-based International Association of Privacy Professionals (IAPP), which *inter alia* offers data protection certifications for "information privacy professionals" (although, like other DPO certification schemes, these do not constitute GDPR-based compliance certifications: see section 2.5.3, below, under the heading "*Formal training and certification [of DPOs]*").

(See the list of DPO associations at the end of this sub-section, with links to their websites.)

The 1995 Data Protection Directive did not yet require the appointment of DPOs by controllers subject to it. Rather, it recognised the existence of DPOs in Member State law and practice, by allowing Member States to exempt controllers from the obligation to notify processing operations to the relevant national data protection authority (DPA), if the Member State's law required the relevant controller to appoint a DPO "*responsible in particular [ ] for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive [and] for keeping [a] register of processing operations carried out by the controller, containing [the same information as would otherwise have to be notified to the DPA]*" (Art. 18(2)).

---

238 The German terms are, respectively: *behördliche-* and *betrieblicheDatenschutzbeauftragter*. For a brief summary of their role and functions under German law, see, e.g.:
https://www.wbs-law.de/eng/practice-areas/internet-law/it-law/data-protection-officer/
For a more detailed exposé in German, see, e.g., Däubler/Klebe/Wedde/Weichert, Kompaktkommentarzum BDSG (Short Commentary on the German Federal Data Protection Law), 3rd. ed. (2010), comments on §4f BDSG, comprising 85 margin notes, pp. 187 – 213.

239 CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations, 30 May 2016, available at:
http://businessdocbox.com/Human_Resources/77901620-Choosing-the-best-candidate-as-your-data-protection-officer-dpo-practical-guidelines-for-organisations.html

However, the 2001 EU regulation setting out the data protection rules for the EU institutions themselves (Regulation (EC) 45/2001)[240]doesrequire each EU institution or -body to appoint at least one DPO (Art. 24). The rules on the EU institutions' DPOs, enshrined in this regulation, are very similar to the ones in the GDPR.

The so-called Law Enforcement Data Protection Directive (Directive 2016/680),[241] adopted at the same time as the GDPR, requires that the "competent authorities" subject to that instrument also appoint a DPO; and the WP29 Guidelines on DPOs (which, as further noted below, contain the main guidance for DPOs appointed under the GDPR) emphasises that "[w]hile these guidelines focus on DPOs under the GDPR, the guidance is also relevant regarding DPOs under Directive 2016/680, with respect to their similar provisions".[242]

The EU-internal DPOs work closely with the European Data Protection Supervisor (EDPS) and have created a Network of Data Protection Officers of the EU Institutions and Bodies. The EDPS created a website, the "DPO Corner" to support them. Following a 2005 position paper by the EDPS,[243] in 2010, the Network issued a set of Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001.[244] In 2012, the EDPS issued a report on the status of DPOs, as part of his monitoring of compliance by the institutions with Regulation (EC) 45/2001.[245] This report "confirms that the DPO function is now well established within EU institutions and bodies, and that they generally comply with Article 24 of the Regulation", but also noted "some areas of concern" which are the subjectof further monitoring by the EDPS.[246] These documents between them contain quite extensive guidance on matters relevant to the appointment, position and tasks of DPOs.

More recently, and more directly relevant to this Handbook, the Article 29 Working Party provided guidelines on DPOs in preparation for the coming into application of the GDPR.[247]The European Data Protection Board (EDPB), which took over from the WP29 upon the coming into application of the GDPR, formally endorsed these guidelines (as well as the

---

240 Full title: Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, O.J. L 8 of 12.1.2001, p. 1ff., available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R0045&from=EN

241 Full title: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89ff., available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

242 Article 29 Working Party Guidelines on Data Protection Officers ('DPOs'), originally adopted on 13 December 2016, as last revised and adopted on 5 April 2017 (WP243 rev.01), p. 4, footnote 2., available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
These are hereafter referred to as "**WP29 Guidelines on DPOs**"

243 EDPS, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, available at: https://edps.europa.eu/sites/edp/files/publication/05-11-28_dpo_paper_en.pdf

244 https://edps.europa.eu/sites/edp/files/publication/10-10-14_dpo_standards_en.pdf

245 EDPS, Monitoring compliance of EU institutions and bodies with Article 24 of Regulation (EC) 45/2001 – Report on the Status of Data Protection Officers, 17 December 2012, available at: https://edps.europa.eu/sites/edp/files/publication/2012-12-17_dpo_status_web_en.pdf

246 *Idem*, p. 3.

247 See footnote 242, above.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

other documents on matters arising under the GDPR, adopted by the WP29 before that date).[248]

As a consequence, several national DPAs have also issued guidance on DPOs, some even before the GDPR, and promoted specific services for them.[249]

The present section of the Handbook draws on the WP29 guidelines in particular, but also refers to the other guidance noted above where appropriate to enrich the thought of the reader.

The main point to make in this introduction to the DPO is that, in terms of the GDPR, it is a crucial new institution that should be seen as an essential means to give practical effect to the "accountability" (duty to demonstrate compliance) principle discussed earlier: where a DPO has been appointed, and dutifully fulfils her tasks (as discussed in part 3 of this handbook), that should result in better, more comprehensive and serious compliance with the GDPR than was achieved through the mainly external supervision by the data protection authorities in relation to the 1995 Data Protection Directive. Now, under the GDPR, DPAs have both a direct, knowledgeable contact point within the organisation of all relevant controllers, and an ally within the controller's organisation. Not surprisingly, several DPAs have made it one of their priorities, now that the GDPR has come into application, to check whether organisations that have to appoint a DPO (as discussed next, in sub-section 2.3.2) have in fact done so.[250]

---

[248] EDPB, Endorsement 1/2018, endorsing *inter alia* the WP29 Guidelines on DPOs (listed as the 7th endorsed document), adopted on 25 May 2018, available at:
https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf

[249] See, e.g.:
Guide de Correspondant Informatique et Libertés (CIL) (*Guide PratiqueCorrespondant*), issued by the **French** Data Protection Authority, the CNIL, in 2011, available at:
https://www.cnil.fr/sites/default/files/typo/document/CNIL_Guide_correspondants.pdf
In **Italy**, the national data protection authority, the *Garante del Privacy*, has issued a set of Frequently Asked Questions (FAQs) on DPOs, available at:
https://www.garanteprivacy.it/garante/doc.jsp?ID=8036793 (FAQs for DPOs in the private sector)
https://www.garanteprivacy.it/garante/doc.jsp?ID=7322110 (FAQs for DPOs in the public sector)
In **Poland**, the national data protection authority, the *UrzqdOchronyDanychOsobowych* (UODO), provides useful tips and recommendations on the application of GDPR on its website in a part dedicated especially to DPOs: https://uodo.gov.pl/p/najwazniejsze-tematy/inspektor-ochrony-danych.
Prior to the entry into force of the GDPR, the Polish authority maintained the ABI website for what used to be called *Administrators of Information Security*. This contained information useful also in preparing future DPOs to perform this function, see: https://abi.giodo.gov.pl/. Through this service, the future DPOs could submit their questions and suggestions regarding the application and interpretation of legal provisions on the protection of personal data.
In the **UK**, the national data protection authority, the *Information Commissioner* (usually referred to as the ICO, which stands for Information Commissioner's Office), provides guidance on its website that essentially reflects (and cross-refers to) the WP29 guidelines, see:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

[250] For instance, the **Swedish** DPA has announced they will be looking into whether organisations in the banking, healthcare and insurance sectors have appointed DPO:s. See
https://www.datainspektionen.se/nyheter/datainspektionen-inleder-forsta-granskningarna-enligt-gdpr/
The **Dutch** DPA similarly stresses in its 2018 – 2019 plan that, *in particular in relation to public authorities*, it will check: "*compliance with the duty to maintain a register of processing operations, the duty to appoint a DPO, and the manner in which the organisation positions the DPO and enables him to fulfil the tasks that he must fulfil under the GDPR*", see:

INTERNATIONAL AND NATIONAL DATA PROTECTION OFFICERS ASSOCIATIONS:

International associations:

Global:

International Association of Privacy Professionals (IAPP):
https://iapp.org/certify/cipp/

European:

Network of Data Protection Officers of the EU Institutions and Bodies:
https://edps.europa.eu/data-protection/eu-institutions-dpo_en

Confederation of European Data Protection Organisations, CEDPO
http://www.cedpo.eu/

National associations:

(The ones marked * are the members of CEDPO)

France:

Association Française des Correspondants à la Protection des Données à Caractère Personnel, AFCDP:*
https://www.afcdp.net/

Ireland:

Association of Data Protection Officers, ADPO:*
https://www.dpo.ie/

Italy:

Associazone Data Protection Officer, ASSO DPO:*
http://www.assodpo.it/en/home_en/

Netherlands:

NederlandsGenootschapvoorFunctionarissenGegevensbescherming, NGFG:*
https://www.ngfg.nl/

Poland:

StowarzyszenieAdministratorówBezpieczeństwaInformacji, SABI:*
http://www.sabi.org.pl/

Spain:

AsociaciónProfesional Española de Privacidad, APEP:*
http://www.apep.es/

UK:

National Association of Data Protection & Freedom of Information Officers, NADPO:
https://nadpo.co.uk/

The **German** and **Austrian** members of CEDPO, respectively the *Gesellschaft für Datenschutz und Datensicherheite.V.*, DGG* (founded in 1977) and *ArgeDaten**, have a wider membership than only DPOs, but are both members of CEDPO:
https://www.gdd.de/ueber-uns
http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=15904tpb

---

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/toezichtkader_autoriteit_persoonsgegevens_2018-2019.pdf (p. 7, under the heading "*Overheid*" (public authority) (our translation).

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

2.5.2 The duty to appoint a Data Protection Officer for public authorities[251]

The appointment of a DPO is mandatory for all public authorities or bodies processing personal data that are subject to the GDPR (Art. 37(1)(a)).[252]While in principle leaving it to the Member States, the WP29 rightly takes an expansive view of this requirement:[253]

> **"Public authority or body"**
>
> The GDPR does not define what constitutes a 'public authority or body'. The WP29 considers that such a notion is to be determined under national law. Accordingly, public authorities and bodies include national, regional and local authorities, but the concept, under the applicable national laws, typically also includes a range of other bodies governed by public law.[254] In such cases, the designation of a DPO is mandatory.

However, the duty to appoint a DPO in fact extends beyond this purely formal category.

> **Private-sector entities that carry out "tasks in the public interests" or that "exercise official authority"**

The WP29 stresses, with reference to the special legal basis for processing in Art. 6(1)(e) GDPR, that (irrespective of the limitations on the duty to appoint a DPO for "purely" private-sector entities)[255] a DPO should also always be appointed by private-sector controllers who carry out "tasks … in the public interest" or who "exercise official authority", even if they are

---

[251] Other than in relation to private entities that carry out "public tasks" or "exercise public authority – as discussed in the text – the duty to appoint a DPO for "purely" private (commercial) companies is not discussed in this Handbook. Suffice it to note that for such entities the Regulation in principle makes a DPO mandatory only in the following instances:

- when the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- when the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 [i.e., of so-called 'sensitive data'] and personal data relating to criminal convictions and offences referred to in Article 10.

(Article 37(1)(b) and (c) GDPR)

These conditions are discussed in some detail in the WP29 Guidelines for DPOs. Here, it may suffice to note that in practice most companies of any size will find it helpful to appoint a DPO to fulfil their "accountability"/ "duty to demonstrate compliance" requirements, discussed above, at 2.2.

[252] The only exception in this regard relates to "courts acting in their judicial capacity" (Art. 37(1)(a) GDPR). However, as the WP29 stresses in its Guidelines on DPOs (footnote 242, above), this does not mean that they need not comply with the Regulation – on the contrary: they too should comply with it. And in respect of processing by courts other than in their judicial capacity, they are subject to the requirement to appoint a DPO.

This Handbook does not deal with DPOs for bodies that carry out processing that is completely outside the scope of EU law, such as national security agencies.

[253] WP29 Guidelines on DPOs (footnote 242, above), p. 6.

[254] See, e.g. the definition of 'public sector body' and 'body governed by public law' in Article 2(1) and (2) of Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public-sector information, OJ L 345, 31.12.2003, p. 90ff. [original footnote]

The English text of this directive is available here:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003L0098&from=EN

[255] See footnote 251, above.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

not formally "public authorities" in terms of domestic law, because in such activities their role will be similar to the role of public authorities:[256]

> A public task may be carried out, and public authority may be exercised not only by public authorities or bodies but also by other natural or legal persons governed by public or private law, in sectors such as, according to national regulation of each Member State, public transport services, water and energy supply, road infrastructure, public service broadcasting, public housing or disciplinary bodies for regulated professions.
>
> In these cases, data subjects may be in a very similar situation to when their data are processed by a public authority or body. In particular, data can be processed for similar purposes and individuals often have similarly little or no choice over whether and how their data will be processed and may thus require the additional protection that the designation of a DPO can bring.
>
> **Even though there is no obligation in such cases, the WP29 recommends, as a good practice, that private organisations carrying out public tasks or exercising public authority designate a DPO.** Such a DPO's activity covers all processing operations carried out, including those that are not related to the performance of a public task or exercise of official duty (e.g. the management of an employee database).

To the examples mentioned by the WP29 one could add the running of prisons and other state institutions or services (such as the deportation of immigrants held to be in a country illegally), by private entities. In all these cases, the private entities effectively act as arms of the state – and in all such cases, the companies in question should appoint a DPO. Member States may further clarify this in their national law, and impose a duty to appoint a DPO on specific controllers or types of controllers other than formal public authorities or bodies (cf. Art. 37(4)).

EXAMPLE:

In **Italy**, the national data protection authority, the *Garante* takes the view that allthe entities that previously fell under the scope of application of Sections 18 to 22 of the Italian Data Protection Code must be considered to be required to designate a DPO. Sections 18 to 22 of the DP Code set forth the general rules applying to processing performed by public entities – such as State administrative bodies, non-profit seeking public bodies at national, regional and local level, regions, local authorities, universities, Chambers of Commerce, health care agencies, independent supervisory authorities, etc. .

The *Garante* also holds that whenever a private entity discharges public functions – e.g. based on a license or concession – designation of a DPO is strongly recommended even though it is not mandatory. It adds, with reference to the WP29 Guidelines on DPOs, that if a DPO is designated on a voluntary basis, the same requirements and conditions apply as in the case of a DPO designated on a mandatory basis – in terms of criteria for the DPO's designation, position and tasks.

[256] WP29 Guidelines on DPOs (footnote 242 above), p. 6, emphasis added. The WP29 use of the terms "public task" and "public authority" is simply a linguistic matter: in the guidelines, these terms refer to the "tasks in the public interest" and "exercise of official authority" mentioned in Art. 6(1)(e)GDPR.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

DPOs for processors

As the WP29 points out, the article in the GDPR that imposes the duty to appoint a DPO in certain cases (Art. 37), as outlined for the public sector above, applies to both controllers and processors.[257] It adds:[258]

> Depending on who fulfils the criteria on mandatory designation, in some cases only the controller or only the processor, in other cases both the controller and its processor are required to appoint a DPO (who should then cooperate with each other).
>
> It is important to highlight that even if the controller fulfils the criteria for mandatory designation its processor is not necessarily required to appoint a DPO. This may, however, be a good practice.

For the public sector, wherein all relevant bodies must in any case appoint a DPO (as discussed above), this may seem to not be a major issue. However, in view of the last comment of the WP29, if a public authority were to sub-contract some processing activity to a private entity (e.g., accounting or the carrying out of surveys) it would be at least advisable to choose a processor that itself also has a DPO, or to require a processor that does not yet have a DPO to appoint one.

To the extent that public authorities working together may also at times act as processors for each other, that should moreover be reflected in the written record of their arrangements, noted under the next sub-heading and further discussed in Part 3, sub-section 3.1.

DPOs for largepublic authorities or groups of authorities

Along with "digital transition", personal data are increasingly processed in highly complex environments and technical architectures, in which different actors work closely together and have joined or linked roles in relation to various processing operations including in relation with citizens. This is also the case in the public sector, which indeed has its own complexities in terms of the measure of autonomy different agencies may have within a broader constitutional or administrative-legal framework. As further discussed in Part 3, section 3.1, one of the first tasks of any newly-appointed DPO must be to "scope" the context for the processing of personal data that she will be responsible for overseeing and/or advising on. Part of this work will be to clarify, with regard to such complex contexts, what precise status the different entities that are part of the complex have, and to make and record suitable arrangements.

In that regard, it should be noted that the GDPR expressly stipulates (as did the 1995 Data Protection Directive) that "where the purposes and means of … processing are determined by Union or Member State law" (as will usually be the case for public authorities) "the controller or the specific criteria for its nomination may be provided for by Union or Member State law" (Art. 4(7)). It will often make sense, in such cases, to appoint the DPO for all the processing covered by such a determination at the offices of the entity that is designated as the controller of the processing. Indeed, the law determining the controller may itself clarify that.

---

257 WP29 Guidelines on DPOs (footnote 242, above), section 2.2, *DPO of the processor*, on p. 9.

258 *Idem*. The WP29 gives some examples, taken from the private sector, that focus on the limitations of the duty to appoint a DPO for that sector; these are therefore not particularly useful in the present Handbook.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

If law does not determine this, the issue may need to be resolved by the relevant government minister, a high official, or between the public entities themselves. This should lead to clear arrangements for the respective responsibilities and competences of different DPOs in different entities forming part of the complex. Part of this involves the decision on where to appoint a DPO, or several DPOs. The arrangements should also cover the links and arrangements between different DPOs in operationally linked entities.

Some very large public bodies (or the government ministers or senior officials of such bodies) may decide to appoint several DPOs for each of its constituent parts – provided this reflects the actual allocation of decision-making powers among the individual departments or units of those large public bodies. Or they may decide to appoint one DPO for the whole body, to work with designated persons in those parts of the whole large entity. In the latter case, it follows from comments made by the WP29 in the context of appointing DPOs on the basis of a service contract (discussed under the next sub-heading) that such designated persons in departments or distinct parts of the large organisation should, on the one hand, fulfil the requirements of DPOs, in particular of not having any conflict of interest, and on the other hand, should be given similar protection as the DPO proper, and not be penalised for the exercise of the DPO-related functions.[259]

Conversely, the GDPR expressly allows for **groups of (formally distinct) smaller public bodies** – such as local authorities (Fr: *communes*) – to decide (or be instructed) to jointly appoint a DPO:

> Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size. (Art. 37(3))

Such a central or common DPO could either be an official of one of the authorities, or it could be decided to jointly engage an external DPO, on the basis of a service contract (as discussed again under the next sub-heading). If one central (in-house or external) DPO is appointed, the other (small) entities should still each designate a staff person responsible for liaising with the central (joint) DPO – and in that case the same applies as was just mentioned with regard to larger authorities: the designated persons should fulfil the requirements of a DPO, and be given similar protection as the DPO proper.

External DPOs

As already noted under the previous sub-heading, public authorities (and private companies) do not have to create an in-house post for a DPO, let alone a full-time one (although many larger bodiesare probably choosing to do so if they have not done so already). Rather:

> [t]he data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract" (Art. 37(6)).

In Germany, where the idea of DPOs originates,[260] law firms or other independent experts offer DPO functions in this way. Moreover, "associations and other bodies representing categories of controllers or processors" can, it would appear, similarly provide DPO functions to their members, and in this respect act on behalf of all of them (cf. Art. 37(4)). This would be useful in particular for small enterprises.A number of major consultancy firms

---

259 Cf. WP29 Guidelines on DPOs (footnote 242, above), section 2.4, last bullet point, on p. 12.

260 See sub-section 2.3.1, above.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

and law firms are also offering DPO support "on the basis of a service contract", and there will also be some smaller firms, especially those specialised in ICT work, that will offer this on such a basis.

However, such external DPOs should not be too far removed from the bodies they provide their services to: as made clear in the next part of the Handbook, DPOs must have a full and intimate understanding of those bodies and their processing operations. They must also be fully and easily accessible – to the staff of the bodies in question as well as to data subjects and data protection authorities (supervisory authorities). Their contact details should be clearly listed on the relevant bodies' websites and in relevant leaflets, etc.

The French data protection authority, the CNIL, feels that a DPO should "preferably" be a member of staff of the organisation of the controller, but accepts that for small- and medium-sized enterprises this may not always be possible.[261]

In the public sector, it may often be preferably to have a DPO from theparticular sector concerned – e.g., as discussed under the previous sub-heading, a central DPO for a large public body or a joint one for a group of smaller authorities attached to one of them – rather than having a private-sector firm acting as external DPO, but this will depend on the culture and practices in the country concerned.

2.5.3 Qualifications, qualities and position of the DPO

Required expertise

The Regulation stipulates that:

> The data protection officer shall be designated on the basis of professional qualities and, in particular, **expert knowledge of data protection law and practices** and **the ability to fulfil the tasks** referred to in Article 39 [as discussed below, at 2.3.4].
>
> (Art. 37(5), emphasis added)

On the first point – expert knowledge – the EU Institutional DPOs' "professional standards" document notes the need for the following:[262]

> (a) Expertise in the area of EU privacy and data protection law, in particular Article 16 of the Treaty on the Functioning of the European Union, Article 8 of the Charter of Fundamental Rights of the European Union, Regulation (EC) 45/2001 and other relevant data protection legal instruments, and expertise in IT and IT Security; and
>
> (b) A good understanding of the way the institution [to which the DPO is appointed] operates and of its personal data processing activities, and an ability to interpret relevant data protection rules in that context.

Technical knowledge of IT systems should be especially emphasised. As the **French** data protection authority, the CNIL puts it:[263]

> In relation to informatics, a good understanding is required of the terminology, [IT] practices and different forms of processing of data. A DPO should be knowledgeable

---

261 CNIL, *Guide PratiqueCorrespondant* (footnote 249, above),p. 6.

262 Network of Data Protection Officers of the EU Institutions and Bodies, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (see footnote 244, above), pp. 3 – 4.

263 CNIL, *Guide PratiqueCorrespondant,* (footnote 249, above), p. 8 (our translation)

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

> about, for example, data management and -exploitation systems, types of software, files and data storage systems, as well as about the requirements of confidentiality and security policies (data encryption, electronic signatures, biometrics, …). This knowledge should enable [the DPO] to monitor the deployment of IT projects and to provide useful advice to the controller responsible for the processing.

Recital 97 of the GDPR also emphasises that:

> The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor.

In other words, the nature of the required "expert knowledge" and "abilities" may vary depending on the activities of the controller: a DPO for a tax authoritywill require different expertise than one working for an educational- or welfare authority. The EDPS refers to this as the need for "**proximity**" (of the DPO to the entity she serves):[264]

> The DPO has a central role within the institution/body: DPOs are [i.e., should be] familiar with problems of the entity where they work (*idea of proximity*) and, given their status, have a crucial role to play in giving advice and help in solving data protection issues [read: as specific to the body in question].

As the WP29 Guidelines on DPOs put it:[265]

> The DPO should also have sufficient understanding of the processing operations carried out [in the relevant sector and organisation], as well as the information systems, and data security and data protection needs of the controller.
>
> In the case of a public authority or body, the DPO should also have a sound knowledge of the [internal] administrative rules and procedures of the organisation.

To which one might add: and of the laws and rules and procedures under which the relevant public body operates (e.g., the Tax Law, or the Law on Education, etc.), and administrative law and procedure generally.

On the other hand, as noted below under the headings "*Conflicts of interest*" and "*Position within the organisation*", appointing someone from the existing staff of a public body may cause problems, especially if the appointee is appointed on a part-time basis and retains other functions within the body in question.

Expert knowledge of data protection law and practices generally can be demonstrated by training and off- or online courses, etc., undertaken by the person in question – such as those offered in the "T4DATA" programme in the context of which this Handbook was written. But many other courses, of varying levels and quality, are also widely offered, as noted next.

---

[264] EDPS, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001 (footnote 243, above), p. 5, emphasis added.

[265] WP29 Guidelines on DPOs (footnote 242, above), p. 11.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Formal training and certification

At the time of writing (December 2018), steps were being taken in one EU Member State, **Spain**, towards the creation of a formal certification scheme for DPOs, but this is not yet operational.[266] Moreover, this certification scheme for DPOs (and some others under consideration) are based on ISO 17024, i.e. on a certification scheme for individuals and professionals; as such, they do not fulfil the requirements of ISO 17065 which is the scheme referred to in the certification concept under the GDPR (certification of services, products, possibly management systems). Thus, the DPO-related certifications are different from "certifications" under Article 42 GDPR. They are commendable but are not GDPR-compliant certifications.

In **France** two "*référentiels*" (in English:"specifications") relating to certifications of DPOs were issued by the DPA, the CNIL, on 11 October 2018 and published in the national Official Journal. One is on the certification related to DPO competence, the other on the stipulation of DPOs' competences and on accrediting organisation authorised to certify DPOs.[267]

In **Germany**, various courses and seminars are offered to train people, some of them leading to some form of certification,[268] but in spite of it being a long-established institution in the country,there is no statutorily-underpinned, officially recognised scheme. Several of the international and national associations of DPOs, listed earlier, also offer specialised trainings – but again, without statutory underpinning.[269]

Many of these training courses or seminars are specifically aimed at providing trainees with expertise in the GDPR, and guidance on the tasks assigned to DPOs under the GDPR. But the GDPR (like German and other national laws) does not specifically provide for any more detailed criteria or certification scheme. Possibly, in future, apart from Spain, other Member States too will provide for such formal, officially recognised schemes, and/or the European

---

[266] The Spanish national data protection authority, the *Agencia Española de Protección de Dato* (AEPD) has established a Certification Scheme for Data Protection Officers (*Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos – Esquema AEPD-DPD*) under which the national Spanish Accreditation Agency (*la Entidad Nacional de Acreditación – ENAC*) can accredit Certification Bodies (*Entidades de Certificación*), that are then allowed to issue the relevant certifications, on the basis of criteria developed by the DPA (AEDP) and a formal exam, see:
https://www.aepd.es/reglamento/cumplimiento/common/esquema-aepd-dpd.pdf (version 1.3, 13 June 2018)
However, no such Certification Bodies have as yet been accredited, and no DPO Certifications have therefore yet been issued.
See also the brief, more general discussion of certification schemes at 2.1, above.

[267] See:
https://www.cnil.fr/fr/certification-des-competences-du-dpo-la-cnil-adopte-deux-referentiels

[268] Cf., e.g.:
https://www.datenschutzexperten.de/grundlagenseminar-ausbildung-betrieblicher-datenschutzbeauftragter-nach-bdsg-mit-dekra.html

[269] The EU institutional DPOs' Standards paper recommends the International Association of Privacy Professionals (IAPP) schemes. IAPP offers region-specific certifications including a Europe-oriented one that specifically also covers the GDPR. See:
https://iapp.org/certify/cippe/
Network of Data Protection Officers of the EU Institutions and Bodies, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (see footnote 244, above), p. 5.
The EU institutional DPOs' paper also mentions IT security management and audit certifications, but these are more general and not specifically aimed at data protection.

Data Protection Board could (presumably informally) endorse some.[270] But until this happens, the parameters remain rather open.As the **Italian** data protection authority, the *Garante*, put it:[271]

> As is the case with all so-called 'unregulated professions', proprietary schemes have been developed to certify, on a voluntary basis, professional skills and competences. Such schemes are managed by several certification bodies. Certifications of this kind – which do not fall under the scope of Article 42 of the GDPR – are sometimes issued following attendance of training and/or learning verification courses.
>
> Though representing a valuable tool that, similarly to other attestations, can provide evidence of a professional's having at least basic knowledge of the applicable rules, such certifications do not equate, per se, to 'qualifications' enabling the discharge of DPO-related tasks and cannot replace the obligation on public administrative bodies to evaluate the requirements a DPO must meet with a view to the tasks and duties set out in Article 39 of the GDPR.

As the Confederation of European Data Protection Organisations (CEDPO) puts it:[272]

> Candidates will probably show you a lot of certificates and diplomas they have gained over the years to show how qualify they are. But how to tell which are valuable and which are not? First thing, you should check is the credentials of the party giving the training and certification. If it is a well-known accredited pan-EU or national organization (in some countries even data protection authorities are certifying), you may feel more comfortable. Also, find out the agenda of the training courses. A one-day event or certifications obtained mainly as a result of a payment and a very simple exam will not have anyone trained into a reliable DPO.

All the various guidance documents also stress the need of organisations to ensure that their DPO can continue to maintain and enhance her or his expertise, also after their appointment, by attending relevant courses and seminars. This is indeed also required by the GDPR (see the last words in Art. 38(2)). As the WP29 puts it:[273]

> DPOs should be given the opportunity to stay up to date with regard to developments within data protection. The aim should be to constantly increase the level of expertise of DPOs and they should be encouraged to participate in training courses on data protection and other forms of professional development, such as participation in privacy fora, workshops, etc.

The **French** data protection authority, the CNIL, usefully provides a special "**extranet**" for registered DPOs, accessible only to them with a username and password, which provides them with legal texts (laws, decrees, etc.) and training and information, including information on new reports or guidance issued by the CNIL, and on other legal and practical developments, and allows them to exchange views and hold discussions.[274]

---

270 The WP29 Guidelines on DPOs (footnote 242, above) merely says that "It is also helpful if the supervisory authorities promote adequate and regular training for DPOs." (p. 11).

271 *Garante del Privacy*, FAQs on DPOs (footnote 249, above), section 3.

272 CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (footnote 239, above), p. 2.

273 WP29 Guidelines on DPOs (footnote 242, above), p. 14.

274 CNIL, *Guide PratiqueCorrespondant* (footnote 249, above), section 4.

Experience

The WP29 Guidelines on DPOs do not address the question of what (length of) experience a DPO should have. However, the Network of EU institutional DPOs recommends that such DPOs should have the following experience/maturity:[275]

> at least 3 years of relevant experience [see below] to serve as DPO in a body where data protection is not related to the core business [*idem*] (and thus personal data processing activities are mainly administrative); and
>
> at least 7 years of relevant experience to serve as DPO in an EU institution or in those EU bodies where data protection is related to the core business or which have an important volume of processing operations on personal data.

They add in a footnote that:

> Relevant experience includes experience in implementing data protection requirements and experience within the appointing institution/organisation resulting in knowledge of how it functions. In the absence of the specified years of experience, the appointing institution/body should be prepared to make more time available to the DPO for training and for work on data protection tasks.

On the issue of whether personal data processing "is related to the core business" of the organisation concerned, the WP29 guidance on the meaning of the similar phrase in the GDPR ("core activities of the controller or processor") is relevant:[276]

> 'Core activities' can be considered as the key operations necessary to achieve the controller's or processor's goals.

The phrase "relevant experience" should not be read as specifically experience as a DPO – it could be experience in the drafting and implementation of policies in the relevant organisation (or a similar organisation), or in relevant areas such as IT, product development, etc.. Suffice it to note that the post should not be assigned to a relatively junior, inexperienced person, or a person not familiar with the particular (type of) organisation in question.

Personal characteristics and qualities

The EDPS, the EU institutional DPOs and CEDPO all rightly note that a DPO must have special personal qualities. He or she is in a delicate position: they must be willing to say "no" to their bosses in rare cases, but more often capable of helping to find a solution to issues that is both acceptable to the organisation and fully compliant with the law (and if anything, privacy-enhancing). As the WP29 Guidelines put it:[277]

> Personal qualities should include for instance integrity and high professional ethics; the DPO's primary concern should be enabling compliance with the GDPR. The DPO plays a key role in fostering a data protection culture within the organisation and helps to implement essential elements of the GDPR …

---

275 Network of Data Protection Officers of the EU Institutions and Bodies, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (see footnote 244, above), p. 4.

276 WP29 Guidelines on DPOs (footnote 242, above), p. 6.

277 WP29 Guidelines on DPOs (footnote 242, above), p. 11.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

The EU institutional DPOs stress the need for the following "personal" and "interpersonal" skills:[278]

> Personal skills: integrity, initiative, organization, perseverance, discretion, ability to assert himself/herself in difficult circumstances, interest in data protection and motivation to be a DPO.
>
> Interpersonal skills: communication, negotiation, conflict resolution, ability to build working relationships.

Elsewhere, they note:[279]

> The proper performance of DPO tasks often requires that the DPO take a firm and insisting attitude also with controllers who have a high position in the organisation, which may be perceived, at best, as bureaucratic or, at worst, unpleasant "trouble-making". Thus, the DPO must be able to withstand the pressures and difficulties which accompany this important position.

CEDPO adds:[280]

> The DPO has to face a number of challenges and with different interests at stake. That is why the DPO should also show strong communication skills combined with refined diplomacy. A DPO is not (and should not be) a "privacy activist": with the support of the other leaders of the organisation, he/she must play a role of a responsible business-enabler and help the organisation to include privacy in the business-decision processes, to not only detect and prevent risks but also create value. In addition, the GDPR requires that his/her reporting line is to the highest level of the management, and that his/her independence is ensured. This requires "gravity" and leadership skills as well.

Independence

We already noted that "[t]he data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract" (Art. 37(6)). However, in neither case is this an ordinary employee- or contractor position. In particular, the Regulation stresses that:

> Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an **independent** manner. (Recital 97)

More specifically, the Regulation stipulates:

> The controller and processor shall ensure that **the data protection officer does not receive any instructions regarding the exercise of those tasks**. He or she **shall not be dismissed or penalised by the controller or the processor for performing his tasks**. The data protection officer shall **directly report to the highest management level** of the controller or the processor.

---

[278] Network of Data Protection Officers of the EU Institutions and Bodies, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (see footnote 244, above), p. 4.

[279] *Idem*, p. 6. The Network makes recommendations to alleviate these pressures in the context of its discussion of the position to be accorded to the DPO in the relevant organisation, as discussed under the heading "*Position of the DPO within the organisation*", below.

[280] CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (footnote 239, above), p. 3 (slightly edited).

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

(Article 38(3))

The WP29 clarifies this as follows:[281]

> [The above stipulations] mean[] that, in fulfilling their tasks under Article 39, DPOs must not be instructed how to deal with a matter, for example, what result should be achieved, how to investigate a complaint or whether to consult the supervisory authority. Furthermore, they must not be instructed to take a certain view of an issue related to data protection law, for example, a particular interpretation of the law.
>
> The autonomy of DPOs does not, however, mean that they have decision-making powers extending beyond their tasks pursuant to Article 39.
>
> The controller or processor remains responsible for compliance with data protection law and must be able to demonstrate compliance.33 If the controller or processor makes decisions that are incompatible with the GDPR and the DPO's advice, the DPO should be given the possibility to make his or her dissenting opinion clear to those making the decisions.

As further noted in Part 3, the DPO's advice – and any actions taken against such advice – should be recorded, and any ignoring of the advice may be held against the controller or processor in any subsequent investigation by the relevant data protection authority. (As noted earlier, conversely, the fact that a controller or processor acted in accordance with any advice or guidance issued by their DPO can constitute an "element" in demonstrating compliance with the GDPR (Recital 77)[282]

The WP29 also clarifies the scope of the stipulation that DPOs "shall not be dismissed or penalised by the controller or the processor for performing [their] tasks":[283]

> This requirement also strengthens the autonomy of DPOs and helps ensure that they act independently and enjoy sufficient protection in performing their data protection tasks.
>
> Penalties are only prohibited under the GDPR if they are imposed as a result of the DPO carrying out his or her duties as a DPO. For example, a DPO may consider that a particular processing is likely to result in a high risk and advise the controller or the processor to carry out a data protection impact assessment but the controller or the processor does not agree with the DPO's assessment. In such a situation, the DPO cannot be dismissed for providing this advice.
>
> Penalties may take a variety of forms and may be direct or indirect. They could consist, for example, of absence or delay of promotion; prevention from career advancement; denial from benefits that other employees receive. It is not necessary that these penalties be actually carried out, a mere threat is sufficient as long as they are used to penalise the DPO on grounds related to his/her DPO activities.
>
> As a normal management rule and as it would be the case for any other employee or contractor under, and subject to, applicable national contract or labour and criminal law, a DPO could still be dismissed legitimately for reasons other than for performing his or her tasks as a DPO (for instance, in case of theft, physical, psychological or sexual harassment or similar gross misconduct).

---

281 WP29 Guidelines on DPOs (footnote 242, above), section 3.3, pp. 14 – 15.

282 See section 2.2.2, above.

283 WP29 Guidelines on DPOs (footnote 242, above), section 3.4, p. 15.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

> In this context it should be noted that the GDPR does not specify how and when a DPO can be dismissed or replaced by another person. However, the more stable a DPO's contract is, and the more guarantees exist against unfair dismissal, the more likely they will be able to act in an independent manner. Therefore, the WP29 would welcome efforts by organisations to this effect.

At the very least, any contract of employment offered to a DPO should include clauses repeating the stipulations on independence in the GDPR, or cross-referring to those. Tribunals or courts adjudicating on cases of dismissal should of course take the provisions of the GDPR fully into account. Where necessary, it may be useful to amend employment laws to that effect. Member States could also underpin the independence of DPOs in other national laws: examples of safeguards against dismissal of certain personnel can be found in laws providing special protections for, e.g., trade union officials, and/or requiring the approval of workers' councils for appointments to and dismissal from certain posts.

NB: The EU institutional DPOs discuss the issues of independence and conflicts of interest (the next issue addressed in this Handbook) mainly in terms of contractual-, length of appointment and other safeguards, as discussed later, under the heading "*Position of the DPO within the organisation*", below. CEDPO merely notes that the organisation that appoints the DPO should "consider … how to ensure the DPO independence".[284]

Conflicts of interest

As the WP29 notes:[285]

> Article 38(6) allows DPOs to 'fulfil other tasks and duties'. It requires, however, that the organisation ensure that 'any such tasks and duties do not result in a conflict of interests'.
>
> The absence of conflict of interests is closely linked to the requirement to act in an independent manner. Although DPOs are allowed to have other functions, they can only be entrusted with other tasks and duties provided that these do not give rise to conflicts of interests. This entails in particular that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case.
>
> As a rule of thumb, conflicting positions may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing.
>
> Depending on the activities, size and structure of the organisation, it can be good practice for controllers or processors:
>
> - to identify the positions which would be incompatible with the function of DPO
> - to draw up internal rules to this effect in order to avoid conflicts of interests
> - to include a more general explanation about conflicts of interests
> - to declare that their DPO has no conflict of interests with regard to its function as a DPO, as a way of raising awareness of this requirement

---

[284] CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (footnote 239, above), p. 3.

[285] WP29 Guidelines on DPOs (footnote 242, above), section 3.5, pp. 15 – 16. The third paragraph ("As a rules of thumb …") appears as a footnote in the document, rather than in the main text, as is done here.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

- to include safeguards in the internal rules of the organisation and to ensure that the vacancy notice for the position of DPO or the service contract is sufficiently precise and detailed in order to avoid a conflict of interests. In this context, it should also be borne in mind that conflicts of interests may take various forms depending on whether the DPO is recruited internally or externally.

The EU institutional DPOs add:[286]

> [T]he DPO should not have conflicts of interest between DPO duties and any other official duties, in particular in relation to the application of the provisions of the Regulation (Art. 24.3). A conflict of interest is present when the other duties, which a DPO is asked to perform, may have directly adverse interests to that of protection of personal data within his/her institution. If necessary, the DPO should raise this matter with his/her appointing authority.

They address the issue in more detail in terms of contractual-, length of appointment and other safeguards, as noted under the next heading. CEDPO again merely notes that, if the DPO appointment is not a full-time job, the organisation that appoints her or him should "consider … how to deal [with] conflict of interest".[287]

Position of the DPO within the organisation

The hierarchical and contractual position of the DPO within an organisation is crucial in relation to ensuring the DPO's effectiveness, independence and avoidance of conflicts of interest.

On the one hand, as noted earlier, the DPO should be "proximate" to the organisation he or she serves (see above, under the heading "*Required expertise*"). Moreover, as CEDPO puts it:[288]

> In order for a DPO to be effective, [she or he] should be on the ground, not only available to various stakeholders within your organization but proactively looking for opportunities to interact with different departments.

This can be problematic in cases of outside DPOs acting under a service contract: they will by definition not be part of the body they assist. In the private sector, there may well be – and in some countries, like Germany, there undoubtedly are – external DPOs with extensive expertise in the private sector or sub-sector in which they work. In the public sector, this may be more difficult (Cf. section 2.3.2, above, under the headings "*DPOs for large public authorities or groups of authorities*" and "*External DPOs*").

But there is always a tension between, on the one hand, the necessary "proximity" of the DPO to her or his organisation, and, on the other hand, the need to avoid conflicts of interest and ensure the DPO's actual independence in practice.

As already noted, in the opinion of the WP29 this means that a DPO cannot be involved in determining the purposes and the means of the processing of personal data, and cannot

---

[286] Network of Data Protection Officers of the EU Institutions and Bodies (CEDPO), Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (see footnote 244, above), p. 15.

[287] CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (footnote 239, above), p. 3,

[288] *Idem*, p. 2.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

hold a senior management position such as chief executive or chief or head of a main department.[289]

The issue is addressed in much more detail by the EU institutional DPOs. Although their views must of course be seen in the light of their specific context, it is still useful to note them. Having noticed various provisions in the regulation that covers them (Regulation (EC) 45/2001)[290] that are designed to guarantee their independence, they continue as follows:[291]

> In practice, however, it may be challenging for the DPO to exercise his/her duties in full independence. Needless to say, the individual situation and personality of the DPO will play a role but it can generally be assumed that certain elements may tend to weaken the position of a DPO:
>
> - A part-time DPO faces a permanent conflict between allocating time and efforts to his/her DPO tasks versus other tasks. With respect to career development and performance review, management may place greater weight on the non-DPO activities. This creates pressure on the DPO to concentrate his/her efforts on the non-DPO tasks. A part-time DPO is also in danger of encountering conflicts of interest.
> - The DPO with a limited contract would likely be in a weaker position to perform his/her DPO duties vigorously than one with a permanent contract (official or temporary agent with indefinite term contract). This is because he/she may be concerned about how his/her actions could negatively influence the renewal of his/her contract. A DPO who is very young and has only limited work experience may have difficulties standing up to controllers, and may be more focused on his/her own career development than on vigorous performance of DPO duties.
> - A DPO who reports to, and is reviewed by, a direct superior in the hierarchy (director or head of unit) may feel pressure to cooperate and get along smoothly with management and other colleagues, as vigorous performance of DPO duties may have a negative impact on career. ... To alleviate this pressure, the DPO should report to, and be reviewed by, the administrative head of the

---

289 See above, under the heading "*Conflicts of interest*", in particular the third paragraph in the quote from the WP29 Guidelines on DPOs. By contrast, the **Italian** data protection authority, the *Garante*, in its FAQs on DPOs, says that:

> … Article 38(3) provides that the DPO 'shall directly report to the highest management level of the controller or processor.' This direct reporting requirement can ensure, in particular, that the top management is informed of the guidance and recommendations provided by the DPO acting in his or her advisory and/or awareness-raising capacity vis-à-vis the data controller or processor.
>
> Accordingly, if an internal DPO is designated it would be preferable, in principle, for a head of department or a senior member of staff to be selected whenever this is feasible based on the organizational structure and taking account of the complexity of processing activities. In that manner, the designated DPO will be in a position to discharge his or her tasks fully autonomously and independently as well as by liaising directly with the top management levels.
>
> (*Garante*, FAQs on DPOs [footnote 249, above], section 2.)

Perhaps the best way to reconcile the views of the WP29 and the *Garante* in this respect, would be to suggest that the DPO should be appointed *at the level of* a head of department or senior manager, but without actually being responsible for data processing operations.

290 See footnote 148, above.

291 Network of Data Protection Officers of the EU Institutions and Bodies, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (footnote 244, above), pp. 6 – 7.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

institution or body. This is particularly important for part-time DPOs, who should report directly to, and be reviewed by, the appointing authority for their DPO duties, and to/by the normal superior in the hierarchy for other duties.

- A DPO who must request staff and resources (IT resources, budget for business trips and training) from his/her direct superior could face difficulties if the latter is not fully committed to achieving data protection compliance. This can be avoided if the DPO has his own budget responsibility, and by having any requests for additional resources subject to approval by the appointing authority.

Best practices to help ensure the independence of the DPO are:

- The institution or body should establish the DPO post within the organisation as one of Adviser, Head of Unit or Director and in any event the DPO position should be officially recognized as management level, on the official organizational chart of the institution/body;
- The institution or body should appoint the DPO for the longest term possible, in light of the DPO's contract. Thus, a five-year appointment should be the norm, unless it is not possible under the circumstances;
- The DPO should have a permanent/undetermined contract with the institution or body [and] should be sufficiently experienced (…);
- The DPO should be able to dedicate his/her time fully to his/her DPO duties, especially for large institutions and bodies, and for smaller ones in the initial phase of establishing a data protection regime. Proper support in terms of resources and infrastructure should be provided. The non-DPO duties of a part-time DPO should not present a conflict of interest, or even the appearance of a conflict, with the DPO duties;
- DPOs in organisations where data processing activities are the core business of the organisation will normally require various staff members. Such staff capacity should be ensured;
- Rules should be in place within the organisation ensuring the obligation of all staff members to cooperate with the DPO without having to wait for an order or permission of their superior;
- The DPO should report to the head of the institution or body, who should be responsible for review of the DPO's performance of his/her duties, as established by the Regulation. The person responsible for the DPO's performance review should be sensitive to the need for the DPO to take strong positions which others in the organization may not appreciate. The DPO should not suffer any prejudice on account of the performance of his/her duties. The appointing authority should ensure that during the DPO's term of office, he/she has at least a "normal" career advancement. When reviewing the DPO's performance, the evaluator should be careful neither to reprimand the DPO for taking unpopular positions nor to consider data protection requirements as an administrative burden. For a part-time DPO, performance on the DPO duties should be given equal weighting to performance on the non-DPO duties. … ;
- The DPO should have his/her own budget line, set up in compliance with the relevant rules and procedures of the respective institution/body; his/her requests for any further resources should be subject to approval by the administrative head. Other arrangements are acceptable if they provide the

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

> DPO with the resources he/she needs to perform his/her mission in an independent manner;
>
> - The DPO should have signing power for DP related correspondence.

DPAs may well feel it appropriate to issue detailed guidance in this respect, on the above lines.

Resources and facilities

The GDPR stipulates that:

> The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 [as listed in section 2.3.4, below, under that heading] by providing **resources necessary to carry out those tasks** and access to personal data and processing operations, and to maintain his or her expert knowledge.
>
> (Article 38(2))

In that regard, the WP29 recommends the following in particular:[292]

- Active support of the DPO's function by senior management (such as at board level).
- Sufficient time for DPOs to fulfil their duties. This is particularly important where the DPO is appointed on a part-time basis or where the employee carries out data protection in addition to other duties. Otherwise, conflicting priorities could result in the DPO's duties being neglected. Having sufficient time to devote to DPO tasks is paramount. It is a good practice to establish a percentage of time for the DPO function where it is not performed on a full-time basis. It is also good practice to determine the time needed to carry out the function, the appropriate level of priority for DPO duties, and for the DPO (or the organisation) to draw up a work plan.
- Adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate.
- Official communication of the designation of the DPO to all staff to ensure that their existence and function is known within the organisation.
- Necessary access to other services, such as Human Resources, legal, IT, security, etc., so that DPOs can receive essential support, input and information from those other services.
- Continuous training. [See above, under the heading "*Formal training and certifications*"]
- Given the size and structure of the organisation, it may be necessary to set up a DPO team (a DPO and his/her staff). In such cases, the internal structure of the team and the tasks and responsibilities of each of its members should be clearly drawn up. Similarly, when the function of the DPO is exercised by an external service provider, a team of individuals working for that entity may effectively carry out the tasks of a DPO as a team, under the responsibility of a designated lead contact for the client.

> In general, the more complex and/or sensitive the processing operations, the more resources must be given to the DPO. The data protection function must be effective and sufficiently well resourced in relation to the data processing being carried out.

As already noted, the EU institutional DPOs feel that "a DPO who must request staff and resources (IT resources, budget for business trips and training) from his/her direct superior could face difficulties if the latter is not fully committed to achieving data protection compliance." They therefore recommend that the DPO be given her or his own budget

---

[292] WP29 Guidelines on DPOs (footnote 242, above), section 3.2, pp. 13 – 14.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

responsibility, with any requests for additional resources being made subject to approval by the appointing authority (rather than such a direct superior).[293]

CEDPO notes:

> [I]n complex organisations, you will need to think whether the DPO will be assisted or not by other people internally who will complement his/her skills, on a permanent basis (the DPO team) or as required from time to time (an external counsel?).

In public authorities the creation of a team would indeed be advisable. In small public bodies, this could consist simply of existing staff regularly meeting with the DPO to discuss relevant matters and prepare policy. In larger ones, some may be more formally assigned part-time DPO supporting functions. In some, it may be necessary to appoint full-timers to support the DPO. As all the guidance documents make clear, the decisions on these matters should be made in the light of (i) the complexity or sensitivity of personal data processing operations and (ii) the size and resources of the entity in question. But in the end, it is a legal requirement of the GDPR that the resources that are allocated to the DPO (and the team) are adequate for the tasks in hand.

DPO powers

Apart from resources, and a sufficiently strong, protected and senior position within the organisation, the DPO also needs to have the power the carry out his or her task. Article 38(2) (quoted under the previous heading) makes clear that to that end the entity appointing the DPO must ensure that he or she will have "access" to personal data and processing operations. This should be read in the same way as the corresponding provision in the regulation covering the EU institutional DPOs, Art. 24(6) of Regulation (EC) 45/2001, is read by those DPOs:[294]

> The Regulation requires controllers to assist the DPO in performing his or her duties and to give information in reply to questions, and states that the DPO shall have access at all times to the data forming the subject matter of processing operations and to all offices, data processing installations and data carriers.
>
> Although the DPO has no enforcement power vis-à-vis controllers, he/she is empowered to monitor compliance by collecting all relevant data, which the appointing institution/body and its controllers are obliged to make available.

Other comments by the EU institutional DPOs in relation to the DPO's duty to ensure compliance with data protection rules are also relevant:[295]

> IT tools may be developed to assist the DPO in performing regular monitoring. Administrative arrangements can also be made, such as ensuring that the DPO receives a copy of all mail raising data protection issues, and requiring that the DPO be consulted on documents raising data protection issues. Careful, regular monitoring of

---

293 See above, under the heading "*Position of the DPO within the organisation*".

294 Network of Data Protection Officers of the EU Institutions and Bodies, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (footnote 244, above), pp. 12. Note that, unlike Art. 38(2) GDPR, Art. 24(6) of Regulation (EC) 45/2001 in fact does not expressly mention access to personal data and personal data processing operations. That is therefore, in the latter context, read into the more general stipulation about providing the necessary resources. This is presumably influenced by the more specific, strong provision on access to such information to be granted (within the EU institutions) to the EDPS.

295 *Idem*.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

> compliance and reporting of results can create a strong pressure on controllers to ensure that their processing operations are compliant. Regular monitoring and reporting are thus the DPO's strongest tools for ensuring compliance. To this end, an annual survey/report issued to the management … is a best practice.

Special issues arise when a controller or processor refuses to follow the advice of its DPO. In the words of the WP29:[296]

> If the controller or processor makes decisions that are incompatible with the GDPR and the DPO's advice, the DPO should be given the possibility to make his or her dissenting opinion clear to the highest management level and to those making the decisions. In this respect, Article 38(3) provides that the DPO 'shall directly report to the highest management level of the controller or the processor'. Such direct reporting ensures that senior management (e.g. board of directors) is aware of the DPO's advice and recommendations as part of the DPO's mission to inform and advise the controller or the processor. Another example of direct reporting is the drafting of an annual report of the DPO's activities provided to the highest management level.

Although there is no specific duty laid down in the GDPR for the DPO to report non-compliance with the law to the authorities, the GDPR does stipulate that it is one of the tasks of the DPO:

> to act as the contact point for the supervisory authority on issues relating to processing, … , and **to consult, where appropriate**, with regard to any other matter (Art. 39(1)(e), emphasis added)

In cases in which a DPO felt that her or his employer was acting in violation of the law, the DPO therefore certainly has the power – and in fact, we would argue, the duty – to raise the issue with the national DPA, to settle the matter. This illustrates the delicacy of the position.

At the same time, as the WP29 rightly emphasises:[297]

> The autonomy of DPOs does not, however, mean that they have decision-making powers extending beyond their tasks pursuant to Article 39.
>
> The controller or processor remains responsible for compliance with data protection law and must be able to demonstrate compliance.

Formalities

All the above requirements etc. of the DPO should be clearly reflected in the legal document by which he or she is appointed. As the Italian data protection authority, the *Garante della Privacy*, puts it in its FAQs on DPOs:[298]

> Article 37(1) of the GDPR provides that a data controller or a data processor shall designate a DPO. Accordingly, existence of an instrument designating the DPO is an integral part of any arrangement to fulfil the relevant obligation.

---

[296] WP29 Guidelines on DPOs (footnote 242, above), p. 15. The same approach is taken by the Network of EU institutional DPOs, see again Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (footnote 246, above), pp. 12 (see the paragraph following the one quoted in the text, above).

[297] WP29 Guidelines on DPOs (footnote 242, above), p. 15, with reference to the "accountability" principle in Art. 5(2) GDPR.

[298] *Garante*, FAQs on DPOs (footnote 249, above), section 1. The *Garante* has attached a **model designation [DPO appointment] form** to the FAQs for convenience. A '**Model form for communicating the DPO's data to the Garante**' is also provided.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

If the candidate DPO is a member of the staff, an ad-hoc instrument designating him or heras DPO will have to be produced. Conversely, if an external entity is selected, the formal designation of that entity as DPO will be an integral part of the ad-hoc service agreement to be drafted pursuant to Article 37 of the GDPR (…).

Regardless of the nature and type of the legal instrument, the latter must specify unambiguously who the DPO will be by mentioning his or her name, the tasks committed (which may also go beyond those envisaged under Article 39 of the GDPR) and the duties related to the support the DPO is expected to provide to the data controller/data processor pursuant to the applicable legal and regulatory framework.

If additional tasks are committed to the DPO on top of those mentioned initially in the designation instrument, either the latter or the service agreement will have to be amended and/or supplemented accordingly.

The designation instrument and/or the service agreement should also specify, in a concise manner, the reasons why the given natural person has been designated as DPO by the public body or authority so that compliance with the requirements under Article 37(5) of the GDPR can be established; to that end, reference can be made to the outcome of the internal or external selection procedure. Specification of the criteria applied prior to designating a certain candidate is not only an indication of transparency and good administration, but also an element to be factored in when assessing compliance with the 'accountability' principle.

Having designated the DPO, the data controller or processor must include the DPO's contact data in the information provided to data subjects and also publish those data on the relevant website(s); communication of the data to the Garante is also required under Article 37(7). As for publication on the website, it may be appropriate to post the DPO's contact data in the 'transparency' or 'openness' section of the site as well as on the 'privacy' page – where available.

As clarified in the[WP29] Guidelines, the DPO's name need not be published pursuant to Article 37(7); however, this might be a good practice in the public sector. Conversely, the contact details must be provided to the Garante in order to facilitate interactions (…) On the other hand, the DPO's contact details must be communicated to the data subjects in case of a personal data breach (see Article 33(3)b.).

2.5.4 Functions and tasks of the DPO (Overview)

In relation to the EU Institutional DPOs, the EDPS has distinguished the following**seven DPOfunctions**:[299]

- Information- and awareness-raising function;
- Advisory function;
- Organisational function;
- Cooperative function;
- Monitoring of compliance function;
- Handling queries or complaints function; and
- Enforcement function.

[299] EDPS, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001 (footnote 243, above), pp. 6 – 7.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

DPOs appointed under the GDPR perform largely similar functions. They correlate to a range of more specific **tasks**, indicated in broad terms in Article 39 GDPR as follows:

Article 39

Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

In practice, DPOs will also naturally become involved in certain tasks that are formally allocated to their controller, in that most controllers (unless they themselves have relevant, in-depth expertise outside the office of their DPO, e.g., in their legal or compliance department) will seek the help of their DPO in performing those tasks. In fact, that is putting it mildly: in many cases, controllers when faced with their new, demanding responsibilities under the GDPR (in particular under the new accountability/demonstrating compliance duties) will look at their DPO to do much of the work involved, even if, as the GDPR expressly makes clear in various respects, in law it remains the controller, and not the DPO, who will be held responsible, and liable, for any failings in this respect.

Specifically, as Article 5(2) GDPR makes clear:

> *The controller* shall be responsible for, and be able to demonstrate compliance with, [the various requirements of the GDPR]

In other words, that responsibility does not rest on the shoulders of the DPO – as is also clear from Article 39, quoted earlier, which emphasises the DPO's advisory and supporting tasks.

However, the DPO is still crucial in that regard, in that she must, through her advice, make it possible for top management, and lower staff, to meet the relevant obligations. Conversely, top- and lower managers have a duty to consult the DPO if issues of GDPR-compliance arise.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

The EDPS has provided a useful, so-called RACI ("**R**esponsible, **A**ccountable, **C**onsulted, **I**nformed") matrix in that regard, applicable in particular in relation to the keeping of records/the register of personal data processing operations:[300]

	Responsible	Accountable	Consulted	Informed
Top Management		**X**		
Business owner	**X**			
DPO			**X**	
IT department			**X**	
Processors, where relevant			**X**	

He added the following clarification of terms:[301]

> '**Responsible'** means having the obligation to act and take decisions to achieve required outcomes; '**accountable'** means to be answerable for actions, decisions and performance; '**Consulted'** means being asked to contribute and provide comments; '**informed'** means being kept informed of decisions made and the process.

The EDPS uses the term "**business owner**" for the person responsible, in practical, day-to-day terms, for the relevant processing activity: the "owner" of the process. As further clarified below, under the heading "*Preliminary task*", it will be part of the DPO's first duties to map out these internal allocations of responsibilities.

In line with the above, in the overview of the DPOs' tasks, below, those tasks will often be described as "helping the controller to ensure" various matters, or as "advising the controller" (or the relevant "business owner"/staff member responsible) on how to achieve certain ends, rather than as "ensuring" those matters or dictating how they should be addressed. In practice, especially in small organisations, it may be that the DPO will carry much of some of these burdens herself, but formally they will remain the responsibility of the controller (and internally, of the relevant "business owner"/staff member responsible).

From the above, and taking this *caveat* about the non-responsibility of the DPO into account, we deduce **fifteen tasks of the DPO, or which will in practice involve the DPO** (plus a *Preliminary task*), which can be grouped under the seven function headings identified by the EDPS, as set out at the beginning of the final part of this handbook, Part Three.

---

300 EDPS, Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments, February 2018, p. 4, available at: https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_1_en_0.pdf One could add to the left column, "Data subjects" and "Data Protection Authority", with "Xs" for them in the last column ("Informed"), but the relevant duties are in fact more complex than could be indicated in that way: the data subjects need to be informed of certain matters in many cases (either by the controller of his own motion or on request), but not always of everything, and the DPA must in some cases not just be informed but actually consulted. In any case, the matrix is aimed at clarifying matters within the controller's organisation, rather than in relation to external entities.

301 *Idem*, footnote 7 (emphases in bold added).

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Suffice it to note here that those functions and tasks, in turn, are clearly and strongly linked to the "**accountability principle**" and the associated "**demonstration of compliance duties**" imposed on the controller, discussed earlier, in section 2.4 of this handbook, above.

In the next part of this handbook (Part Three), we provide guidance on how the controller and the DPO should perform those tasks. First, however, it is important to reiterate that – although the DPO will have major influence and input in relation to the above tasks, she does not have any personal formal responsibility for compliance with the GDPR.

Of course, the DPO will have to establish a strategy in order to be able to accomplished all of the tasks, according to an agenda by year or semester with some flexibility with regard to possible unexpected issues arising (such as a sudden data protection problem or a personal data breach affecting the organisation, or the DPA deciding to investigate her organisation).

- o – O – o –

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

PART THREE

Practical guidance on the tasks of the DPO or that will in practice involve the DPO

("The DPO Tasks")

This part of the handbook seeks to provide practical guidance on **thetasks of the DPO, or that will in practice involve the DPO,** already listed in section 2.5.4, above, and again set out below. For the sake of brevity, we will from time to time refer to them as "The DPO Tasks". As noted in that section, the fifteen tasks are derived from the list of tasks set out in broad terms in Article 39 GDPR, grouped under **the seven functions of the DPO**, identified by the EDPS. In the various sections discussing the task, we provide **examples** illustrating them, relating to actual practice.

The DPO's tasks:

Preliminary task:

Scoping the controller's environment

Organisational functions:

Task 1: Creating a register of personal data processing operations

Task 2: Reviewing the personal data processing operations

Task 3: Assessing the risks posed by the personal data processing operations

Task 4: Dealing with operations that are likely to result in a "high risk": carrying out a Data Protection Impact Assessment (DPIA)

Monitoring of compliance functions:

Task 5: Repeating Tasks 1 – 3 (and 4) on an ongoing basis

Task 6: Dealing with personal data breaches

Task 7: Investigation task (including handling of internal complaints)

Advisory functions:

Task 8: Advisory task – general

Task 9: Supporting and promoting "Data Protection by Design & Default"

Task 10: Advise on and monitoring of compliance with data protection policies, joint controller-, controller-controller- and controller-processor contracts, Binding Corporate Rules and data transfer clauses

Task 11: Involvement in codes of conduct and certifications

Cooperation with and consultation of the DPA:

Task 12: Cooperation with the DPA

Handling data subject requests:

Task 13: Handling data subject requests

Information and raising awareness:

Task 14: Information and awareness-raising tasks

Task 15: Planning and reviewing the DPO's activities

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Preliminary task:

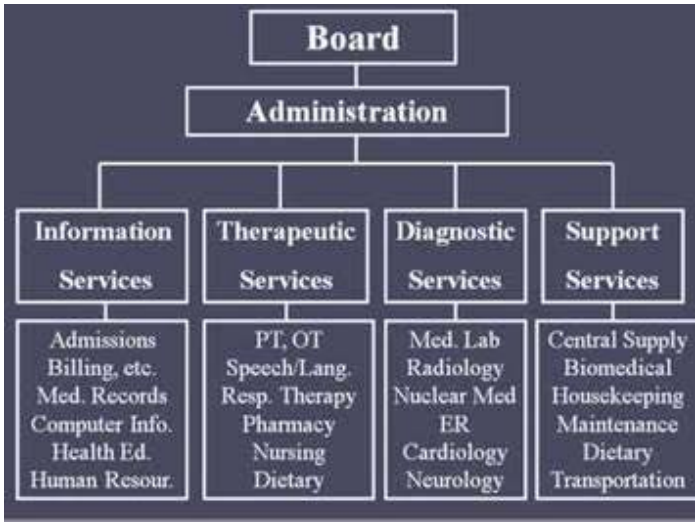
Preliminary task of the DPO: scoping the controller's environment & mapping the organisation's processing activities in broad terms

A DPO can only carry out her tasks in relation to her employer if she is fully cognisant of (i) the **internal** distribution and allocation of tasks and responsibilities in relation to (or which may involve) any processing of personal data; (ii) the **external** links and arrangements of that organisation with other organisations; and (iii) the **legal**framework(s) for those.

Prior to undertaking her main other tasks – except for the carrying out of the initial inventory (register) of personal data processing operations, listed first under the next heading (Task 1), which can be done in parallel – the DPO must therefore map those internal and external links and lines of responsibility in relation to all and every personal data processing operation, and put those in the wider context of her organisation's role and aims, and thoroughly familiarise herself with the relevant rules.

To clarify the **internal** structures and roles, the DPO must first of all obtain and study the **organogram** of her organisation, which management should be able to supply her with.

EXAMPLE: Organogram of a hospital



Source: *Principles of Health Science*, https://www.youtube.com/watch?v=FpQEwbAV3Qw

However, organograms will usually only identify the relevant units and departments in the most general of terms: "human resources", "finance and accounts", "legal", "customer management", etc. (with many public bodies adopting the terminology of private entities, e.g., by referring to welfare claimants as "customers" of the welfare office). They are a useful starting point, but little more than that. In in-depth discussions with senior management, including the organisation's legal and ICT officer(s) and, where appropriate, regional or national offices, the DPO should clarify in more detail what exactly the different units and departments are responsible for, including in particular for what purposes each of the units and departments needs, and actually processes, personal data; under what architecture of internal and external technologies this is done; and whether this involves any external technological services or means (including cloud computing). This is where the preliminary scoping overlaps with the carrying out of the inventory of personal data processing operations in Task 1 – but at the preliminary stage, the relevant personal data

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

processing operations need only be identified in broad terms, with reference to the purpose for each such operation, and the technologies used. Moreover, the DPO should at this preliminary phase also already obtain an initial idea of what exact **tasks** and **responsibilities** each unit or department has in respect of each personal data operation – i.e., she should identify who is the "**business owner**" of each operation (to the use the EDPS's terminology).

EXAMPLES:[302]

The **Spanish** data protection authority, the AEDP, list the following as **examples of official (statutorily required) personal data registers maintained by local authorities**:

- Population register
- Register of people liable to pay local taxes
- Register of recipients of benefits (e.g., housing benefit or disability benefit)
- Register of clients of social services (e.g., child welfare)
- Registers of imposition of fines (e.g., parking fines)
- Register of permits and licences issued (e.g., to run a bar)
- Register of local police units and officers
- Register of people signed up with local authorities' employment bureaux;
- Register of children in local education
- Register of people issued with official documents (e.g., births, marriages, deaths)
- Register of people buried in local cemeteries
- Register of users of libraries run by the local authorities
- Register of people who have signed up to receive notifications about cultural events

As well of course as:

- Accounts
- Human resources
- Etcetera

The data protection authority provides the following **examples of laws or regulations underpinning the processing of personal data in relation to some of the personal data registers maintained by Spanish local authorities**, given above:[303]

Register:	Underpinning law/regulations:
• Population register	Law on local population registers
• Register of people liable to pay local taxes	Law on local *haciendas*
• Human resources data	Regulations covering this activity

In some circumstances, there may be other legal bases for the processing, e.g.:

Register:	Other legal bases:
• Register of people signed up to cultural events	Consent & local regulation
• Register of users of local authorities' libraries	Contract & local regulation

[302] Based on: *Protección de Datos y Administración Local* (Data Protection and Local Administration) a sectoral guide issued by the Spanish data protection authority, AEPD, 2017, p. 8 (our translation and edit), available at: https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf

[303] AEPD, Sectoral Guide on Data Protection and Local Administration (previous footnote), p. 11.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

In addition, it is important that at this stage the DPO (with the help of IT and security staff) also thoroughly familiarises herself with **the technical ICT systems, -architecture and -policies of her organisation**: the computers (or where they still are used, the manual filing systems) used and whether these include portable and/or mobile devices (and/or personal "own devices" of relevant staff – for which a "Bring Your Own Device [BYOD] policy has to be [put] in place); whether PCs or devices are used online or only offline, on-site or also off-site; what security software and encryption is used, and whether it is fully up-to-date; what the external links and facilities are (including the use of cloud servers, especially if they are based outside the EU/EEA, e.g., in the USA – in which case the relevant data transfer arrangements and contracts need to be checked); whether any of the processing is done by processors (in which case the contracts with them will need to be reviewed);[304] what the physical security measures are (doors, rooms, network- and PC passwords, etc.); whether security policies and training is in place; etc., etc. At this preliminary stage those many issues need not all be addressed and resolved – but they should at least be **noted, mapped and recorded**.

Next, the DPO should try to clarify all the **external** links that her organisation has to other organisations. Those generally come in **two types**: (a) the (sister/mother/daughter) organisations that the DPO's organisation has formal links with, within what will (in the public sector) usually be an overall **hierarchical framework**. A local authority may be formally under the immediate jurisdiction of a regional body, which in turn is under the control or supervision of a provincial or federal state body, that at the highest level fits within a wider country-wide public agency, under a national ministry. However, there will be major differences in the arrangements from country to country, or even within a country, including as concerns the relative autonomy that the various bodies have, also in relation to the establishment and management of their personal data processing operations – this is exactly why the DPO should thoroughly familiarise herself with the particular arrangements for her particular organisation.

The framework for all the relevant public bodies belonging to a certain hierarchy will be largely defined in **formal law**, at a range of levels: constitution, statute law, statutory instruments (secondary, binding legislation), ministerial ordnances and instructions, as well as in possible non-binding or non-statutorily-underpinned **administrative arrangements**,

[304] The Spanish data protection authority, AEPD, in a contribution to this handbook, gives as **examples** of processing operations that are often outsourced by local authorities (i.e., in which, in data protection terms, the processing is done by a processor):
• The preparation of the staff payrolls [*continues overleaf*]
• The destruction of documentation or media
• The control of video surveillance cameras
• Tax collection management
• Maintenance of computer equipment
• Data processing of the Municipal Population Register:
• Data processing of municipal taxes:
• Processing of human resources data: applicable to public service regulations.
• The subscription through a service offered by a City Council on its website to receive communications related to cultural activities.
• Enrolment in a job bank.
(The AEDP also notes cloud computing, as already noted in the text.)

agreements,[305] guidance and policy statements, etc. The processing of personal data by the DPO's organisation may also be covered by a **code of conduct**, of which there are various types. Again, the DPO should acquire as full and detailed an understanding of those rules and arrangements and codes – and of the processes through which they are adopted, applied and reviewed and amended – as possible, again if needs be with the help of the legal officer(s) of her organisation (and/or by attending courses on the relevant issues if she is not fully cognisant of these issues when taking up her position).

There will also be other DPOs in the other organisations belonging to the relevant hierarchy – and it will be crucial for our" DPO to become fully engaged with them, in a **DPO network**. Where there is as yet no such network, the DPO should work towards its creation. All the DPOs should of course establish **close and good links with the national data protection authority (DPA)**, including any senior staff members within the DPA with specific responsibilities in relation to public authorities/the kind of public authority to which the DPO's organisation belongs.

The arrangements made by the French data protection authority, the CNIL, for a national network of DPOs, with a dedicated "extranet", is a good example of a DPA supporting such networking and interactions.[306]

Then there are links to **external organisations that are outside of the DPO's organisation's hierarchy**. Those can include other **public authorities in a different hierarchy** – for instance, there can be links between educational establishments and welfare institutions, or the police, or between educational authorities in one country and similar organisations in another. Again, there will be (or ought to be) **laws** covering such links with such bodies, or other **formal, binding arrangements and agreements** (such as data sharing arrangements and agreements between educational institutions and welfare organisations). The DPO should again obtain full details of all such arrangements whenever these involve or may involve the processing of personal data – and should indeed review them, to see if they adequately reflect, confirm and implement the requirements of the GDPR and of any relevant national data protection laws and -rules – and indeed of more general human rights law.[307] The DPO may not be able to challenge a deficient law or legal arrangement as such, but could – and should – notify her employer, and probably the relevant DPA, of her view that the law is deficient.

Sometimes, the links between, and the cooperation between, formally distinct entities are based on **informal, non-public arrangements**. However, this is problematic from a data protection point of view.

---

[305] Those agreements could include agreements between public bodies under which one public body processes personal data on behalf of another public body, i.e., acts as a processor for the latter body. See the discussion in the text of controller-to-controller-, controller-to-processor- and data transfer contracts.

[306] See section 2.3.3, under the heading "*Formal training and certification*", above, and footnote 456, below.

[307] Cf. the European Court of Human Rights judgment in *Copland v. the UK* of 3 April 2007, in which the Court held that a vaguely-phrased provision in a law granting a public authority broad competence in a certain area (*in casu*, the provision of higher and further education) did not constitute "law" in terms of the European Convention on Human Rights:
http://hudoc.echr.coe.int/eng?i=001-79996 (see in particular para. 47.)

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

As the Article 29 Working Party noted in its opinion on the concepts of controller and processor:[308]

> [There is] a growing tendency towards organisational differentiation in most relevant sectors. In the private sector, the distribution of financial or other risks has led to on-going corporate diversification, which is only enhanced by mergers and acquisitions. In the public sector, a similar differentiation is taking place in the context of decentralisation or separation of policy departments and executive agencies. In both sectors, there is a growing emphasis on the development of delivery chains or service delivery across organisations and on the use of subcontracting or outsourcing of services in order to benefit from specialisation and possible economies of scale. As a result, there is a growth in various services, offered by service providers, who do not always consider themselves responsible or accountable. Due to organisational choices of companies (and their contractors or subcontractors) relevant databases may be located in one or more countries within or outside the European Union.

This leads to difficulties in relation to division of responsibilities and the attribution of controlship. The Working Party said the entities involved should provide "sufficient clarity" about this division of responsibilities and effective attribution of (various forms and levels of) controlship – which in practice means that the entities involved should ***discuss*** these matters, ***agree*** on these divisions and attributions, and ***record*** this in the form of a **formal arrangement** that can (and on request of course should) be provided to the relevant DPA or DPAs and (perhaps in simplified form) to data subjects and the general public.

As part of the preliminary scoping task, the DPO should again **check** whether any such formal arrangements are in place, and if so, whether they (a) really reflect the practical divisions and attributions of responsibilities and (b) fully meet the requirements of the GDPR. If there is no formal arrangement in place, the DPO should **advise** that one be drawn up urgently (and she should be involved in the discussion, agreement and recording). If only informal arrangements are in place, the DPO should **advise** that they be replaced by formal ones.

Moreover, when the links and arrangements with other entities amount to or include controller – controller and/or controller – processor arrangements, those should be underpinned by relevant (GDPR-compliant) **controller – controller and/or controller – processor contracts**; and when the links and arrangements with other entities involve transfers of personal data to non-EU/EEA countries (so-called "third countries"), the transfers should be based on relevant (GDPR-compliant) **data transfer clauses** (either standard clauses approved by the relevant DPA or DPAs or by the EDPB, or *ad hoc* clauses that conform to the GDPR).

Where such contracts or clauses are in existence, the DPO should **review** them to see if they comply with the GDPR, and where there are no such contracts or clauses, but there should be, the DPO should **advise** that they be concluded urgently.

These tasks of the DPO in relation to formal agreements, controller – to controller- and controller – to processor contracts and data transfer clauses (and in other related respects)

---

[308] Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (WP169, adopted on 16 February 2010), p. 6, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

are further discussed at 3.x, below. Here, it will suffice to note that the DPO should **identify** such issues in the preliminary scoping task, to then be addressed thereafter.

Finally, the DPO's organisation will have **links with external (private- and public-sector) suppliers of goods or services**, ranging from outsourced data processing, accounting and website management to the supply of canteen meals, maintenance and repairs, staff medical and wellbeing support, etc., etc. The work done in these respects will be based on **contracts** (either ordinary civil contracts or special public-private contracts). Those contracts will also be the basis for – and ought to specifically address – any processing of personal data by the parties to those contracts: for the collecting of the relevant personal data to the sharing and use of those data, to their final destruction or erasure. If the other entity is a controller in its own right, those contracts (or at least the data protection-relevant elements of those contracts) will, in data protection terms, constitute **controller-to-controller personal data processing contracts**. If the other entity acts merely as a processor for the DPO's organisation, the contract will be a **controller-processor contract**. And if under the contract personal data are transferred to a place outside the EU/EEA (typically, to a "cloud" server maintained by the contractor), those contracts constitute **personal data transfer contracts**.

In the preliminary scoping exercise, the DPO should again **identify** whether there are such contracts, and then, shortly after the scoping exercise, **review** them, and where they are missing or deficient in GDPR terms, **advise** that they should be drawn up or revised.

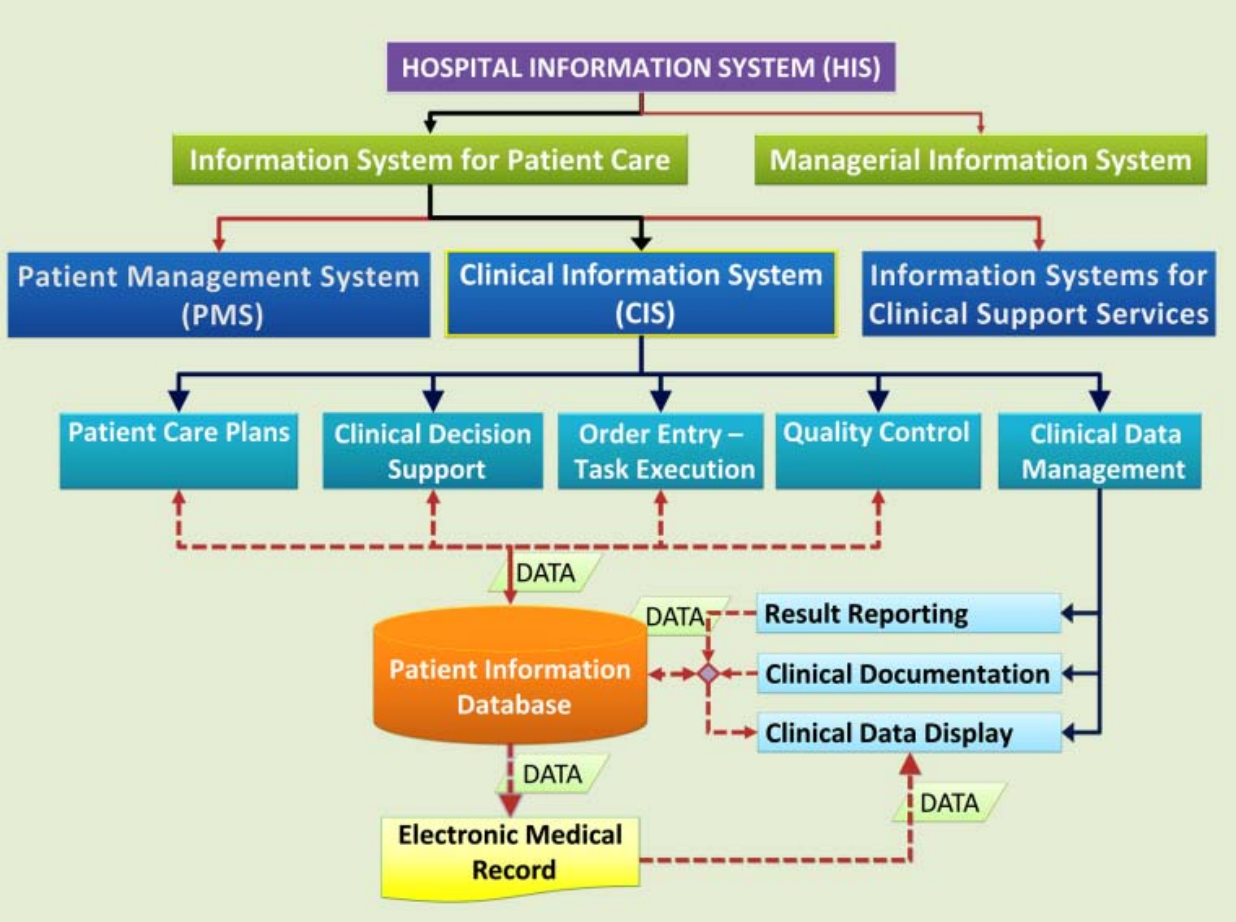
Mapping the organisation's processing activities in broad terms

Once the DPO has carried out the general scoping of her organisation (as set out above), she will be able to map the organisation's personal data processing activities in broad terms, as a crucial step towards the creation of a detailed register of all those activities and all the individual personal data processing operations, carried out in Task 1 (discussed next). This should lead to a chart such as the one provided overleaf, by Dr.Abdollah Salleh, setting out the "*Functional Components of a Clinical Information System*" (used in the first T4DATA training, in a presentation by the Italian data protection authority, the *Garante del Privacy*).[309]

[309] Luigi Carrozzi, presentation to the first "T4DATA" training session, June 2018, slides on "*Practical Guidance for DPOs – The register of data processing operations*".

EXAMPLE:

Map of an organisation's [here: a hospital's] personal data processing activities



Source: Dr Abdollah Salleh, https://drdollah.com/hospital-information-system-his/

Note that the above map is more closely related to personal data processing operations than the organogram of a hospital, provided earlier.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Organisational tasks:

TASK 1: Creating a register of personal data processing operations

Subject to a limited exemption discussed below under that heading, under Article 30 GDPR, each controller must "maintain a **record** of processing activities under its responsibility", listing various details of each operation such as the name of the controller (and, one may add, of the "business owner") of the operation, the purpose(s) of the operation, the categories of data subjects, personal data and recipients, etc. This duty to keep a register of processing operations is closely linked to the accountability principle, discussed at 2.2, above, by facilitating effective supervision by the relevant data protection authority ("supervisory authority") – as is underlined by Recital (82) of the GDPR:[310]

> ***In order to demonstrate compliance*** with this Regulation, the controller or processor **should maintain records of processing activities** under its responsibility.
>
> Each controller and processor **should be obliged to cooperate with the supervisory authority and make those records, on request, available to it**, so that it might serve for monitoring those processing operations.

In other words, as the Italian data protection authority, the *Garante*, puts it:[311]

> **[The register is a] measure to demonstrate compliance to GDPR**

The reference to "processing operations under [the controller's] responsibility" suggests that the record (often also referred to as register) must cover **all** such processing operations, and this is indeed expressly stipulated in the German version of the GDPR.[312] This also makes sense because, as the *Garante* also points out:[313]

> The overall picture of information assets "personal data" and the related of processing operation provided by the register, is **the first step to accountability** since it enables the evaluation of risk on rights and freedom of individuals and to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

Although, as with most other requirements of the GDPR, this is formally a duty of the controller rather than the DPO, in practice it will be the DPO who will either be in charge of this work (in close cooperation with the controller's relevant staff), or who will at the very least be closely involved in it and oversee it. As the Article 29 Working Party (WP29) put it:[314]

> In practice, DPOs often create inventories and hold a register of processing operations based on information provided to them by the various departments in their organisation responsible for the processing of personal data. This practice has been

---

310 Luigi Carrozzi, presentation to the first "T4DATA" training session, June 2018, slides on "*Practical Guidance for DPOs – The register of data processing operations*

311 *Idem*.

312 "*JederVerantwortliche und gegebenenfalls sein VertreterführeneinVerzeichnis**allerVerarbeitungstätigkeiten**, die ihrerZuständigkeitunterliegen.*" (emphasis added).

313 Luigi Carrozzi (footnote 236, above) (original emphasis).

314 WP29, Guidelines on DPOs (footnote 242, above), section 4.4, *The DPO's role in record-keeping*, p. 18.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

established under many current national laws and under the data protection rules applicable to the EU institutions and bodies.[315]

Article 39(1) provides for a list of tasks that the DPO must have as a minimum. Therefore, nothing prevents the controller or the processor from assigning the DPO with the task of maintaining the record of processing operations under the responsibility of the controller. Such a record should be considered as one of the tools enabling the DPO to perform its tasks of monitoring compliance, informing and advising the controller or the processor.

In any event, the record required to be kept under Article 30 should also be seen as a tool allowing the controller and the supervisory authority, upon request, to have an overview of all the personal data processing activities an organisation is carrying out. It is thus a prerequisite for compliance, and as such, an effective accountability measure.

For a new DPO, this requires first of all the (overseeing of the) carrying out of an **inventory** of all the processing operations of the organisation that may involve the processing of personal data and of links with other organisations. This involves considering what data do constitute such data – which is not always straight-forward.[316]

An ***initial, basic inventory*** can usefully be carried out in parallel with the broader scoping of the organisation and its operational context, in the preliminary task (Task 0), described above. Subject to the exemption, noted below, this should then be followed by a ***full inventory***.

The ***full inventory*** should lead to the creation of the **register** (the collection of "**records**") of all of the controller's personal data processing operations, mentioned in Article 30 (as discussed a little later in this section, under the heading "*Contents and structure of the register entries*") – which should thereafter (and after the review and assessment noted next, in Tasks 2 and 3) be kept up-to-date by the DPO (or the DPO should at least ensure that it is kept up to date): see the text below, under the heading "*(ongoing) Monitoring of compliance*", after Task 4.

Exemption:

Article 30(5) exempts **enterprises and organisations that employ fewer than 250 persons, and that only process personal data "occasionally"**,[317] from the duty to maintain a record of their personal data processing operations. However, this exemption does not apply if:

- the processing that the enterprise or organisation carries out is "*likely to result **in a risk to the rights and freedoms of data subjects***" (note that this does not have to be a "high risk", such as triggers the need to hold a Data Protection Impact Assessment (Task 4): any risk to the rights and freedoms of data subjects, however small, would require the recording (and reviewing) of the controller's operations;
- the processing is **not occasional**; or

315 Article 24(1)(d) Regulation (EC) 45/2001 [original footnote]

316 See WP29, Opinion 4/2007 on the concept of personal data (WP136), adopted on 20 June 2007, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

317 In our view, the condition that the small organisation must only carry out personal data processing "occasionally" follows from the stipulation (discussed in the text) that the exemption does not apply if the processing by the small organisation is "not occasional".

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

- the processing includes **sensitive data or data on criminal convictions and offences**.

As to the first of these, in the context of DPIAs (which are required when there is a likelihood of a "*high risk* to the rights and freedoms of natural persons": see Task 4, below), the WP29 has described the term "**risk**" as:[318]

> a scenario describing an event and its [negative] consequences, estimated in terms of severity and likelihood –

and explained that:[319]

> the reference to "**the rights and freedoms**" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

In April 2018, the WP29 issued a "Position Paper" on Article 30(5) GDPR.[320] In this, it stressed that:

> the wording of Article 30(5) is clear in providing that the three types of processing to which the derogation does not apply are alternative ("or") and the occurrence of any one of them alone triggers the obligation to maintain the record of processing activities.
>
> Therefore, although endowed with less than 250 employees, data controllers or processors who find themselves in the position of either carrying out processing likely to result in a risk (not just a high risk) to the rights of the data subjects, or processing personal data on a non-occasional basis, or processing special categories of data under Article 9(1) or data relating to criminal convictions under Article 10 are obliged to maintain the record of processing activities. However, such organisations need only maintain records of processing activities for the types of processing mentioned by Article 30(5). For example, a small organisation is likely to regularly process data regarding its employees. As a result, such processing cannot be considered " occasional" and must therefore be included in the record of processing activities.[321] Other processing activities which are in fact "occasional", however, do not need to be included in the record of processing activities, provided they are unlikely to result in a risk to the rights and freedoms of data subjects and do not involve special categories of data [so-called "sensitive data"] or personal data relating to criminal convictions and offences.

Example:

In **Croatia**, detailed information on all civil servants and employees of public bodies must by law be uploaded to a central system, the *Public Sector Employee Register*. This also applies

---

318 WP29 Guidelines on DPIAs (footnote 351, below), p. 6.

319 *Idem*, emphasis added.

320 WP29, Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR, 19 April 2018, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045
The Position Paper was not expressly endorsed by the European Data Protection Board when it endorsed a range of more formal "Opinions" of the WP29 (EDPB, Endorsement 1/2018, see footnote 248, above), but can still be regarded as authoritative on the issue.

321 The WP29 considers that a processing activity can only be considered as "occasional" if it is not carried out regularly, and occurs outside the regular course of business or activity of the controller or processor. See WP29 Guidelines on Article 49 of Regulation 2016/679 (WP262). [original footnote]

to even the smallest public entities, such as small local communities that may employ only a very few people. The processing of the data on these few employees by that very small community is therefore not "occasional" and does not benefit from the record-keeping exemption.

If in doubt, the controller should seek the advice of the DPO on these questions – and the DPO should be inclined to advise in favour of creating a full record in marginal cases, rather than risk the organisation being held to have breached the duties enshrined in Article 30(1) – (4).

Notes:

1. On the question of whether the register of personal data processing operations must be made accessible to anyone (online or otherwise), or not, see Task 12, "*Information and awareness-raising tasks*".
2. The creation of the register as such does not yet involve an assessment of the compliance of the registered operations with the GDPR: that is done in Task 2 – but of course, the register should be amended and updated as and when changes are made to the processing operations recorded in it: see the entry "*Monitoring of compliance: Repeating Tasks 1 – 3 (and 4) on an ongoing basis*", at the end of Task 4 (just before Task 5).

Contents and structure of the register entries (records):

The GDPR distinguishes between the registers of controllers and processors.

Contents and structure of the controller register entries (records)

Under Article 30(1) GDPR, the **register** of personal data processing operations of a *controller* is to consist of a collection of **records** of each such operation; and **each such record must include the following details** (words in square brackets and italics added):

a. the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
b. the purposes of the processing;
c. a description of the categories of data subjects and of the categories of personal data [*including whether any of the data fall within the list of "special categories of data"/sensitive data*];
d. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
e. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
f. where possible, the envisaged time limits for erasure of the different categories of data;
g. where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

This list does not include the **legal basis** for the processing of the relevant data (Article 6 in relation to non-sensitive data; Article 9 in relation to sensitive data), or legal instruments used for the contracts with processors, or for data transfers – but these are such crucial issues in relation to any determination of the legality and GDPR-compatibility of any processing operation that they too should be recorded in the register, in relation to each

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

personal data processing operation (defined by reference to the purpose of the processing), with the validity of the claimed and recorded legal basis checked in due course.

SAMPLE FORMAT OF A BASIC CONTROLLER PERSONAL DATA PROCESSING RECORD[322]

Note that a separate record must be created for each distinct operation

Part 1 – Information about the controller etc.

CONTROLLER CONTACT DETAILS: Name, Address, Email, Telephone	
JOINT CONTROLLER CONTACT DETAILS:* Name, Address, Email, Telephone	
REPRESENTATIVE CONTACT DETAILS:* Name, Address, Email, Telephone	
(*) *If applicable*	
DATA PROT'N OFFICER CONTACT DETAILS: Name, Address, Email, Telephone	

Part 2 – Basic information on the personal data processing operation (PDPO)[323]

1.	Name of the PDPO[324]	
2.	Unit responsible ("business owner")	
3.	Purpose of the PDPO	
4.	Categories of data subjects	
5.	Categories of personal data	
6.	Does this include sensitive data?	
7.	Legal basis for the processing:* * Cf. Art. 6 GDPR for non-sensitive	

[322] Expanded from the template form presented by Carrozzi (footnote 236, above) with edits (e.g., portrait rather than landscape format) and entries about the name of the operation, the legal bases for the processing, suitable safeguards for data transfers and details relating to technologies and security added (in line with further recommendations by Carrozzi).
NB: A sample format of a more detailed (15-page) personal data processing record is attached at the end of the discussion of the present task.

[323] The sample chart above is merely intended to illustrate the recording requirements in broad terms. The **sampledetailed personal data processing record** mentioned in the previous footnote and attached to this Task asks for crucial further detail, e.g., for each category of personal data: the purpose, relevance and source of the data, etc..

[324] From a data protection-legal perspective, any personal data processing is operation is best defined on the basis of the purpose served by the operation (as recorded at 2.). However, in many organisations, the people performing the operations will often have a specific functional/internal name for the operation – although the two designations will of course often overlap and can be identical.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

data, Art. 9 for sensitive data	
8. Are the data transferred to a 3rd country or an international organisation?	
9. In case of transfers referred to in the 2nd subparagraph of Article 49(1) GDPR: what suitable safeguards are provided?	
10. Time limits for erasure	
11. Details of systems, applications and processes (paper/electronic files; desktop suite/centrally managed application/ cloud service/local network; data transmissions; etc.) and related technical and organisational (security) measures	
12. Does the processing involve the use of (a) processor(s)? If so provide full details and a copy of the relevant contract(s).	

Contents and structure of the processor register entries (records)[325]

Under Article 30(2) GDPR, the **register** of personal data processing operations of a *processor* is to consist of a collection of **records** of each such operation; and **each such record must include the following details**:

a. the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

[325] Note that it is increasingly difficult to fully distinguish processors from controllers. Often, entities that used to provide straight - forward processor services (acting purely as instructed by the controller, who determined the means and purposes) now take on many more responsibilities and may become "joint controllers". This is especially the case in relation to providers of cloud services – some of which now even offer "*Artificial Intelligence and Machine Learning (AI/ML) via Machine-Learning-as-a-Service (MLaaS)*", see: http://www.techmarketview.com/research/archive/2018/04/30/machine-learning-as-a-service-market-overview-technology-prospects
As discussed in the *Preliminary Task*, the arrangements between entities involved in such complex arrangements should be clearly and properly recorded. The forms recording the relevant processing operations should be reviewed and amended to fit in with these (agreed and recorded) inter-entity arrangements. Entities that are more than straightforward processors should use the detailed form mentioned in the next footnote.

b. the categories of processing carried out on behalf of each controller;

c. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

d. where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Below, we again provide a sample format of the kind of record a processor should keep to meet these requirements.

SAMPLE FORMAT OF A PROCESSOR'S PERSONAL DATA PROCESSING RECORD[326]

Note that a separate record must be created for each distinct personal data processing operation for each distinct controller

Part 1 – Information about the processor and any sub-processor(s)

PROCESSOR CONTACT DETAILS:	Name, Address, Email, Telephone
DATA PROT'N OFFICER CONTACT DETAILS:	Name, Address, Email, Telephone
SUB-PROCESSOR CONTACT DETAILS:*	Name, Address, Email, Telephone
DATA PROT'N OFFICER CONTACT DETAILS:	Name, Address, Email, Telephone
SUB-PROCESSOR CONTACT DETAILS:*	Name, Address, Email, Telephone
DATA PROT'N OFFICER CONTACT DETAILS:	Name, Address, Email, Telephone

* *If applicable*

Part 2 – Information about the controller of the specific PDPO in question

CONTROLLER CONTACT DETAILS:	Name, Address, Email, Telephone
JOINT CONTROLLER CONTACT DETAILS:*	Name, Address, Email, Telephone
REPRESENTATIVE CONTACT DETAILS:*	Name, Address, Email, Telephone
(*) *If applicable*	
DATA PROT'N OFFICER CONTACT DETAILS:	Name, Address, Email, Telephone

NB: The relationship between the controller and the processor, and between the processor and any sub-processor, must be based on a written contract meeting the requirements of Article 28 GDPR. Processors should keep copies of the relevant contracts with the filled-in form.

326 Again expanded from the template form presented by Carrozzi (footnote 236, above) with edits.

Part 3 – Details of the personal data processing operation (PDPO)

1. The category (kind of) of processing that is carried out for the controller in relation to the overall PDPO, including:	
- the categories of data subjects;	
- the categories of personal data; and	
- whether this includes sensitive data.	
2. Are the data transferred to a 3rd country or an international organisation?	
3. In case of transfers referred to in the 2nd subparagraph of Article 49(1) GDPR: what suitable safeguards are provided?	
4. Details of systems, applications and processes used (type of electronic files; desktop suite/centrally managed application/ cloud service/local network; data transmissions; etc.) and related technical and organisational (security) measures	
5. Does the processing involve the use of (a) sub-processor(s)? If so provide full details and a copy of the relevant contract(s).	

Contents and structure of the register:

The DPO should build up the **register** from the **records** she receives on each distinct personal data processing operation. They are normally best sorted by **organisation**, and within that by **business owner**. With each individual record the DPO should keep all the relevant documentation (as indicated in the template forms, above).

The DPO should note in the register when each record was received, when the relevant processing operation was reviewed (as is done in Task 2, described next), with the outcome

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

of that review and any remedial measures taken; and indicate when the operation should be due for the next regular (e.g., annual) review.

- o – O – o –

Attached: Sample format of a detailed personal data processing record[327]

[327] A more detailed template personal data record is also provided by the Polish DPA, the *UrządOchronyDanychOsobowych* (UODO) on its website, in Polish, at: https://uodo.gov.pl/pl/123/214 (follow the first link at the bottom of the page.)

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Attachment:

SAMPLE FORMAT OF A DETAILED PERSONAL DATA PROCESSING RECORD

Please use a separate form for each distinct personal data processing operation

NB: If you feel you need to elaborate or clarify a matter, please add a number in the relevant field and attach a page with those elaborations or clarifications, with reference to that number.

I. GENERAL: * indicates a mandatory field (if applicable)

Controller: (Main controller entity)* (Name, place of establishment & address, registration number, etc.)	
Associated entities (Any entities with which the controller is linked in relation to this operation, e.g., mother/daughter companies or linked public bodies; processors that are involved in this operation)	
Business Unit: ("Business owner")* (E.g., HR, Accounts, R&D, Sales, Customer Support)	
Contact person within the unit:	
PRIMARY PURPOSE OF THE PERSONAL DATA PROCESSING OPERATION:* ***Please specify as precisely as possible***	
Are the personal data used or disclosed for any other (secondary) purpose or purposes?* ***Please specify as precisely as possible and add link or reference to the associated record.***	
Is this operation performed for all associated entities alike? Or separately and/or differently for different entities?* ***Please specify.*** ***If the operations are different for the different entities, please use separate forms for each.***	
Roughly, to how many individuals (data subjects) does this operation relate (if known)?*	[*Add number or "not known"*]
Date of submission of this form to the DPO:*	
Form & processing operation reviewed by DPO:	[*Yes/No and date to be entered by the DPO*]
Due date for revision/update of this form:	[*To be specified by the DPO*]

(CC) Douwe Korff & Marie Georges/Final Text as approved – 190723

II. DETAILS OF THE PERSONAL DATA PROCESSING OPERATION:

II.1 The data and the data sources [NB: All fields are mandatory if applicable, unless otherwise indicated]

1. What personal data or categories of personal data are collected and used for this operation?	*Tick √ as appropriate:*	**When, how and from whom are the data obtained?** **E.g.:** (data subject=DS) - DWP, upon employing the person - DS, upon enrolment in research
- Given & Family Name(s)		
- Date of Birth		
- Home address		
- Work phone number		
- Private phone number		
- Work email address		
- Private email address		
Add any further data, below if applicable:* ** See also below, at 2,* re *sensitive data*		
Add further rows if necessary		
2. Do the data you collect and record for the operation <u>include or indirectly reveal</u> any of the following special categories of personal data ("sensitive data")?	*Tick √ if the data is expressly collected and used for the operation;* *Tick √ and add ("Indirect") if the datum is indirectly revealed (explain in a note if necessary)*	**When and from whom are the data obtained?** **E.g.:** (data subject=DS) - DWP, upon employing the person - DS, upon enrolment in research
- Race or ethnic origin		
- Political opinions or affiliations		
- Religious or philosophical beliefs		
- Trade union membership		
- Genetic data		
- Biometric data		
- Data concerning the		

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

person's health		
- Data concerning the person's sexual orientation or sex life		
- Information on criminal convictions or offences		
- National identifier* * E.g., NI Number, Tax Number		
- Data about debts/credit score		
- Data on minors		
3. If this is known or determined: How long are the (special and other) data retained? What happens then?* * Indicate period or event, e.g., "7 years" or "Until 5 years after termination of employment". Also explain what happens to the data, e.g., erasure/destruction or rendered anonymous. **NB: If there are different retention periods for different data, please indicate that.**		

II.2 Disclosures of data

4. To what third parties are which of the above data disclosed? And for what purposes? **NB: This also applies to the data being made accessible, especially directly, online** ***Re* disclosures involving transfers to third countries, see further below, at II.5**	**Recipient third party and place and country of establishment:**	**Purpose(s) of the disclosure(s):**
ALL THE DATA LISTED AT II.1		
***OR:* The following data:** (Copy the data from 1 & 2, above)		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		

(CC) Douwe Korff & Marie Georges/Final Text as approved – 190723

-		
-		
-		
-		
-		
-		
Add further rows if necessary		

II.3 Legal basis for the processing

5. **On what legal basis are the data processed?** **NB: <u>If there are different legal bases for different data or for different (primary, secondary or new, unrelated) purposes, please indicate that (if needs be by copying and pasting the lists of data from above to below, with the different legal bases moved to the second column)</u>.**	*Tick the relevant legal basis and provide clarification in the next column as relevant.*	**Clarification:**
- The data subject consented to the processing **NB: See also QQs 6 – 9, below.**		
- The processing is necessary for the contract between your organisation and the data subject (Or in order to take steps at the request of the data subject prior to entering into a contract – e.g., obtaining references)		
- The processing is necessary for compliance with a legal obligation that your organisation is subject to * E.g., employment or tax law – *please specify the law in question*		
- The processing is necessary in order to protect the vital interests of the data subject or of another person		
- The processing is necessary for the performance of a task carried out in the public interest * * *Please specify the source of the task (typically, a law)*		
- The processing is carried out in the exercise of		

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

official authority ** Please specify the source of the task (typically, a law)*		
- The processing is necessary for a legitimate interests of your organisation (or another entity) and is not outweighed by the interests of the data subjects E.g., marketing to your own clients, or fraud prevention – please spell out.		
CONSENT – further detail:		
6. **If the data are processed on the basis of the consent of the data subjects, how and when is this consent obtained?** **NB: If the consent is provided in paper or electronic form, please provide a copy of the relevant text/link**		
7. What proof is kept of the consent having been given? E.g., are copies kept of paper forms, or logs of electronic consent?		
8. How long is this proof retained?		
9. If in the context of a contract, more data are asked for by your organisation than are necessary for the contract, is the data subject told s/he does not need to provide the additional data? **NB: Either say "N.A.", or if this applies, provide a copy of the relevant text/link**		

II.4 Informing of the data subjects [NB: This information is not mandatory but Is helpful in assessing and revising internal data protection policies]

10. **Are the data subjects informed of the following? And if so, when and how?**	*Indicate Yes/No (or "N.A.")* **NB: If relevant, you can say "Is obvious in the context" and/or "The data subject already had this information"**	Explain when and how this is done **Please provide copies of any information notices or links**
- That your organisation is the controller of the personal data processing operation?		

- Details of your organisation (e.g., name and registration number)?		
- If applicable, details of your representative in the EU?		
- The contact details of the DPO?		
- The main purpose of the processing?		
- Any further purpose for which your organisation wants (or may want) to process the data?		
- If the data were not obtained directly from the data subjects, the source or sources of the data, and whether those included publicly accessible sources (such as public registers)?		
- The recipients or categories of recipients of the data? **NB: Cf. Q4, above**		
- Whether the data are (to be) transferred to a non-EU/EEA country (*e.g., to a cloud server in the USA*)? **NB: This also applies to the data being made accessible (especially directly, online) to entities in non-EU/EEA countries.**		
- If the data are so transferred, what safeguards have been put in place, and where the data subjects can obtain copies of those? **NB: Safeguards can be provided in data transfer contracts or through privacy codes or privacy seals.**		
- For how long the data will be retained?		
- Of their rights to demand access, rectification or erasure of their data; to		

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

ask for their data to be blocked; to object to processing?		
- Of their right to lodge a complaint with the relevant Data Protection Authority?		
11. If all or part of the data are processed on the basis of consent, are the data subjects informed of the following?		
- That they can withdraw their consent at any time (and how to do that) (without that affecting the lawfulness of the prior processing)?		
12. If the provision of the data is a statutory or contractual requirement (or a requirement for the entering into a contract), are the data subjects informed of the following?	*Indicate Yes/No (or "N.A.")* **NB: If relevant, you can say "Is obvious in the context" and/or "The data subject already had this information"**	Explain when and how this is done **Please provide copies of any information notices or links**
- Whether they are required to provide the data, and what the consequences are if they do not provide them?		
13. **If all or part of the data are processed on the basis of the "legitimate interest" criterion, are the data subjects informed of what the legitimate interest in question is?**		Please provide a brief summary of the criteria applied in the balancing test performed with regard to the data subjects' fundamental rights and freedoms as per Article 6(1)f GDPR.
14. **If the data subjects will be the subject of automated decision-making or profiling, are they informed of the following?**		Please provide a brief summary of the logic used in the automated decision-making or profiling.
- That such decision-making or profiling will take place?		
- In broad (but meaningful)		

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

terms, what "logic" is involved?		
- What the significance of the automated decision-making or profiling is and the envisaged consequences of the decision-making or profiling?		

II.5 Transborder data flows [NB: An entry in field 17 is not mandatory, but again useful for internal evaluation]

15. **Are any of the personal data transferred to a third [i.e., non-EU/EEA] country (or a sector in a third country) or to an international organisation that *has* been held to afford an "adequate" level of protection under Art. 45 GDPR?**	*Indicate Yes/No and the country/ies in question. If the transfer is of only some but not all of the data, specify for each category of data.*	*Explain the purpose of the transfer, e.g.: as part of your organisation's own operations (e.g., in using cloud-based software), or as part of a disclosure of the data to a third party (please specify that party/those parties)*
ALL THE DATA LISTED AT II.1		
***OR:* The following data:** (Copy the data from 1 & 2, above)		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
Add further rows if necessary		

16. **Are any of the data transferred to a third [i.e., non-EU/EEA] country (or a sector in a third country) or to an**	*Indicate Yes/No and the country/ies in question. If the transfer is of only some but not all of the data, specify*	*Explain the purpose of the transfer, e.g.: as part of your organisation's own operations (e.g., in using cloud-based*	*What safeguard or derogation underpins the transfer? Please provide a number as per*

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

international organisation that has not been held to afford an "adequate" level of protection under Art. 45 GDPR?	*for each category of data.*	*software), or as part of a disclosure of the data to a third party (please specify that party/those parties)*	*the list in the* ****Note*** *below and provide a copy of any relevant document*
NB:*If data are transferred for different purposes to different recipients in different countries, please answer the questions separately for each transfer context.*			
ALL THE DATA LISTED AT II.1			
OR: **The following data:** (Copy the data from 1 & 2, above)			
-			
-			
-			
-			
-			
-			
-			
Add further rows if necessary			

*** NOTE:** Under the GDPR, transfers to countries that have not been held to provide "adequate" protection may only take place if "appropriate safeguards" are in place, as listed in the left column, below, or if a derogation applies, as listed in the right column.

Safeguards as per Art. 46 GDPR: 1. International instrument between public authorities; 2. Binding Corporate Rules (BCRs); 3. Approved standard data transfer clauses; 4. Code of Conduct; 5. Certification; 6. Approved ad hoc clauses	Derogations as per Art. 49 GDPR, if safeguards as per Art. 46 are not available (see EDPB Guidelines in this respect: restrictive application and interpretation are mandated): 7. Consent; 8. Contract between controller and data subject 9. Contract between controller and third party 10. Necessary for important reasons of public interest 11. Necessary for legal claims; 12. Necessary to protect vital interest of data subject or others; 13. Transfer is made from a register accessible to the public

17. **Are rules in place to deal with any judgment of a court or tribunal and any decision of an administrative authority of a third country that may be served on the controller or any processor, requiring the controller or processor to transfer or disclose personal data?** (Cf. Art. 48 GDPR)	*Indicate Yes/No and if yes, please provide a copy of the guidance.*

(CC) Douwe Korff & Marie Georges/Final Text as approved – 190723

III. SECURITY AND CONFIDENTIALITY

NB: If the answers to the questions below differ for different data, please answer them separately for each distinct data set.	*Please provide details:*
Are the personal data listed at II.1 held on paper or in electronic format? If on paper, are they held in a structured manual collection (data file)?	
Where (physically) are the data stored? (Your offices? At servers at the main controller? At servers of a linked organisation? At servers of a third party (e.g., a Cloud Service Provider)?	
What measures are in place to protect against unauthorised access to the physical place(s) where the data are stored/accessible? Is there a data security policy in place that regulates this? (*If so, please provide a copy*.)	
What hardware is used in the processing of the data? Who is responsible for the management and security of this hardware?	
Are (any of) the data stored on removable media/devices? What are those media/devices? Who is in possession of them?	
Can any of the people with access to the data use personal devices to access or process the data? If so, is there a BYOD policy on this? *Please provide a copy of the policy.*	
Are all the persons authorised to access the personal data subject to a duty of confidentiality (be that under a statutory or professional set of norms or under contract)? *Please provide details or copies of any relevant norms or contract clauses.*	
What software/applications is/are used in the processing of the data? (E.g., desktop MS Office suite, centrally managed application, cloud service, etc.)	

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

- Is this software managed locally or centrally? If centrally, who is the central entity? If that is not you, is there a formal arrangement between that entity and your organisation as to the use of the software? *Please provide a copy of this arrangement.*	
- Does the software use a "cloud"? If so, who is the Cloud Service Provider, and where is that provider legally based? And where is/are the cloud server/s physically based? Are the data on the cloud server fully encrypted? How (i.e., using what encryption technology)? *Please provide a copy of the contract under which this processing takes place.*	
- Who is responsible (i.e., who has "admin" authority) in relation to this software? (You? Someone else within your organisation? Someone in a central entity with which you are linked? Anyone else?)	
Are the data at any time/in any circumstances electronically transmitted to another medium, system or device?	
If they are electronically transmitted, is this done: - over the Internet? If so, are the data encrypted? How (i.e., using what encryption technology)? - by means of FTP? How is this secured? - by means of a VPN? How is this secured? - other – *please specify*	

- o – O – o -

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

TASK 2: Reviewing the personal data processing operations

For the DPO, after having created the register of her organisation's personal data processing operation (Task 1), the next step is the carrying out of an in-depth **review** of all the registered personal data processing operations, to see whether they meet the requirements of the GDPR in all relevant respects, including in respect of:

- purpose-specification and -limitation;
- the validity of any consent (and the existence of documentary proof of consent having been given) or the applicability of any other legal basis for the processing;
- personal data processed and their relevance and necessity in relation to the specified purpose(s));
- data quality (accuracy, up-to-dateness, etc., of the data, as well as data minimisation and pseudonymisation);
- information provided to the data subject of the controller's own motion (either when data are collected from the data subject or otherwise, or on request – also in relation to data collected from website visitors);
- the length of time for which the data are retained in identifiable form and any information as to de-identification;
- technical, organisational and physical data security (including physical access limitation and technical access limitation [user name, passwords, PINs policies, etc.], encryption, etc.);
- cross-border data transfers (and the legal and other contractual or other arrangements for them);
- etcetera.

In the light of the findings on the above, the DPO should be able to **assess**:

- whether the processing operation ***as a whole*** can be said to comply with the overriding principle of lawfulness and fairness.

(Note that this GDPR-compliance assessment is separate and different from the risk assessment, described below as Task 3).

The records of the individual personal data processing operations created in Task 1 (in particular if created in the more detailed format)[328] should form the basis of the review, in that they will lead to the DPO asking and answering of relevant questions including, specifically:

- Is it sufficiently clear which entity is the **controller** of the personal data processing operation, and if any other entities are involved, what their respective status is (e.g., ***joint controller***, ***processor***, or separate ***third party*** controller)? If this is not obvious, are **formal arrangements** in place that clarify these issues (cf. Task 1, above)?
- Is it sufficiently clear which business unit is the "**business owner**" in respect of the personal data processing operation (i.e., which has day-to-day *de facto* responsibility

[328] As provided for in the sample format of a detailed personal data processing record attached to Task 1.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

for the processing)? Is this set out in a **formal document** (e.g., specific instructions from the controller to the unit)?

- Is the **purpose**, or are the **purposes**, of the personal data processing operation specified in sufficiently precise terms? Where (i.e., in what kind of **document**)? If the personal data used in the processing operation are used for more than one purpose, what is the ***primary purpose*** and what is or are the ***secondary purpose(s)***? Are those secondary purposes ***compatible*** with the primary purpose, or are they separate purposes?

  NB: In assessing the compatibility of any processing for any secondary purpose with the primary purpose, the DPO must take into account the matters listed in Article 6(4) GDPR.

  Are all the purposes for which the personal data are processed fully justified and legitimate?

- Are the personal data that are processed **adequate**, **relevant** and **necessary** for the primary purpose? How is it ensured that they are and remain **accurate** and **up to date** for this purpose, and what arrangements are made to ensure this and to ***rectify*** or ***up-date*** or ***erase*** inaccurate or out of date information?

  Are the measures taken adequate and sufficient? Would it be possible to achieve the same purpose with less risk to the privacy and other rights of the individuals concerned?

- What personal data are used or disclosed for any secondary purposes or indeed new, unrelated purposes (typically, to a third party)? Are the personal data that are processed **adequate**, **relevant** and **necessary** for those secondary or new, unrelated purposes? (If all the data collected for one [primary] purpose are disclosed unthinkingly for a/any secondary purpose or purposes or a new, unrelated purpose, they, or some of them, may well be excessive for that secondary or unrelated purpose or those secondary or unrelated purposes. Has this been considered?)

  NB: Cf. the detailed personal data processing form, at II.2.

  Are all the secondary purposes for which the personal data are processed fully justified and legitimate?

- How is it ensured that the data that are used or disclosed for secondary or new, unrelated purposes*are***accurate** and **up to date** for those secondary or new purposes at the time of first use or disclosure for those purposes, and what arrangements are made to ensure they *remain***accurate** and **up to date** after that first use or disclosure, and are ***rectified*** or ***up-dated*** or ***erased*** as and when they become inaccurate or out of date? Are the relevant measures adequate and sufficient?

  NB: If the data are used or disclosed for more than one secondary or new purpose, these questions should be answered separately for each separate secondary or new use or disclosure.

- **When, how, from whom and in what form** are **which** of the personal data obtained? E.g.: the data subject, a government department, a (former) employer, etc.; e.g., on paper, by electronic transfer, etc.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

NB: This question should be answered for both **non-sensitive** and **sensitive data**, and if different data are obtained from different sources, this should be indicated. Cf. the detailed personal data processing form, at II.1 and II.2.

Are those sources appropriate? Could some data that are obtained from third parties perhaps be better asked of the data subjects themselves?

- **How long** are the personal (non-sensitive and sensitive) data **retained**? **What happens at the end of that period**? (E.g.: ***erasure***, ***destruction***, ***rendering the data anonymous*** – or ***pseudonymous*** – but note that the latter means the data are still retained in identifiable form).[329] If the data are retained in anonymous or pseudonymous form, ***why*** is that done? (E.g., for research or historical purposes? If so, the processing for that purpose should be separately assessed for compatibility with the GDPR.)

  NB: The retention period can be specified as a specific time or as an event, e.g., "7 years" or "Until 5 years after termination of employment". Note that there are **formal standards** on the recommended methods of data erasure/destruction for different categories of data and data carriers.[330] The DPO should check whether those are followed (especially as concerns sensitive information in either the data protection-legal sense or in a broader social or political sense.

  Are the data retention periods appropriate? Or too long? Are the data erasure/destruction measures in accordance with national and international standards? If data are retained beyond the normal retention periods in anonymised or pseudonymised form: (i) is this appropriate in view of the purpose of the extended retention? Could data retained in pseudonymised form be retained in fully-anonymised form and still be sufficient for the special purpose? How true is any claim that any data are "anonymised"? (Note that full anonymisation is increasingly

---

329 Note that under the GDPR (as under the 1995 Data Protection Directive) personal data can only be said to have been rendered anonymous if they can no longer be linked to a specific individual by *anyone* – i.e., not just by the controller (**but also, e.g., by colleagues or relatives or friends who might find the data if released in supposedly de-identified form on the Internet or in discarded paper).** In that regard, DPOs should be aware that more and more data that might seem to be "non-personal" or that are said to have been "rendered anonymous" can increasingly easily be (re-)linked to specific individuals. In particular, data in supposedly "anonymous" "Big Data" datasets are often unexpectedly, and worryingly, re-identifiable, especially if different datasets are linked or "matched". Furthermore, if even truly non-personal datasets are used to create "profiles" (be that of typical consumers of a particular product, or typical patients, or typical criminals or terrorists), and those profiles are then applied to datasets to single out individuals that meet the profile – then that processing too can very seriously affect those individuals, who may be denied insurance, or a job, or access to a flight or even a country (or worse) on the basis of effectively unchallengeable algorithms. See: Douwe Korff and Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, report for the Council of Europe Consultative Committee on data protection, June 2015, Council of Europe document T-PD(2015)11, section I.iii, *The dangers inherent in data mining and profiling*, available at:
https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf

330 See for example:

- DIN German Institute for Standardization, Office machines - Destruction of data carriers, DIN 66399, October 2012.
- NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization, December 2014, at http://dx.doi.org/10.6028/NIST.SP.800-88r1
- US National Security Agency/Central Security Service, Media Destruction Guidance, at https://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml

difficult to achieve, especially in large data sets and more especially if data sets are allowed to be matched or linked to other data sets.)

- To what **third parties** are which of the above data **disclosed**? And **for what purposes**? Are the data that are disclosed ***adequate***, ***relevant*** and ***necessary*** for those purposes, ***accurate*** and ***up to date***, and if so, how is it ensured that they remain so?

  NB: The answers to the above may in part cross-refer to the answers to the earlier questions, above.

- On what **legal basis/bases** are the personal data processed?

  NB:

  For non-sensitive data, the legal basis must be one of those specified in Article 6 GDPR, for sensitive data, one of those specified in Article 9 GDPR.

  Note that the "legitimate interest" basis for processing (Art. 6(1)(f)) does not apply to processing of any data – including non-sensitive data – by public authorities in the performance of their tasks (Art. 6(1), final sentence) and cannot be relied upon by any controller, whether in the public- or private sector, to process sensitive data (cf. Art. 9).

  Moreover, if the processing is based on Article 6(1)(c) or (e) ("processing [that] is necessary for compliance with a legal obligation to which the controller is subject", "processing [that] 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"), this must be based on Union or EU Member State law (Art. 6(3)). If either of those is the indicated legal basis, the DPO must check whether the law in question meets the requirements set out in Article 6(3) GDPR.

  Is the claimed legal basis appropriate for the processing? Are the relevant conditions for the application of the legal basis met (e.g., as concerns consent, as further addressed below)?

  Note that the legal basis for processing for the primary purpose may be different from the legal basis for any processing (including use or disclosure) of any of the data for any secondary or new, unrelated purpose(s) – and the validity of the claimed legal basis must be assessed separately for each of those.

- If the data are processed on the basis of the **consent** of the data subjects:
  - ***how and when*** is the consent obtained (e.g., in paper or electronic form, by a direct question or by asking an individual to tick a box)?[331]
  - what ***proof*** is kept of the consent having been give (e.g., paper copies, logs)?
  - how and for how long is this proof ***retained***?
  - if in the context of a contract, more data are asked for by your organisation than are necessary for the contract, is the data subject ***told s/he does not need to provide the additional data***?

[331] Note that a simple statement on a website that says: "*By continuing to use this website, you consent to the collection and use of your personal data*" is no longer sufficient to constitute valid consent under the GDPR. Not only is there insufficient information on the use of the data – which renders the "consent" invalid as it is not "informed consent". But also, it is doubtful whether continuing on the website as such can be said to constitute an "*unambiguous indication of the data subject's wishes*" to so consent (cf. the definition of consent in Art. 4(11) GDPR).

- Are the **data subjects informed** of all the matters of which they should be informed (see Article 13 and 14 GDPR, as reflected in the detailed personal data processing form, at II.4), and if so, when and how?

  Is all the relevant information provided? Is that done in the best format? At the best time? Are mandatory fields clearly distinguished from optional ones?

- Are any of the data **transferred to a third [i.e., non-EU/EEA] country** (or a sector in a third country) or to an **international organisation** that *has* been held to afford an "adequate" level of protection under Art. 45 GDPR?

  Does the relevant adequacy decision indeed cover the processing? Is it still valid (cf. the finding by the CJEU that the "Safe Harbor" adequacy decision was invalid)?

- Are any of the data **transferred to a third [i.e., non-EU/EEA] country** (or a sector in a third country) or to an **international organisation** that has **not** been held to afford an "adequate" level of protection under Art. 45 GDPR? If so, what safeguard or derogation underpins the transfer?

  NB: Under the GDPR, transfers to countries that have not been held to provide "adequate" protection may only take place if *either* "**appropriate safeguards**" are in place, as listed in Article 46 GDPR, *or* if a **derogation** applies, as listed Article 48 GDPR (cf. section II.5 in the detailed personal data processing form, question 16).

  Is/are the safeguard(s) or derogation(s) mentioned correct? Does it/do they meet all the requirements as listed in the relevant article (Art. 46 or 48)?

- Are rules in place to deal with any judgment of a court or tribunal and any decision of an administrative authority of a third country that may be served on the controller or any processor, requiring the controller or processor to transfer or disclose personal data?

  NB: Under Article 48 GDPR, judgments and decisions of third countries "may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter." This is a difficult matter to assess for business owners and many controllers and processors, and guidance should be in place on how business owners and controllers and processors should act if faced with such a judgment or decision. At the very least, processors and business owners should immediately refer the matter up to the highest management level of the controller, and the DPO.

  If there is relevant guidance, is it adequate (e.g., if it was adopted prior to the entering into full application of the GDPR, it may not have mentioned involving the DPO in the matter, as there may not have been a DPO when the guidance was drawn up)? If there is as yet no guidance on this, it should be drafted as a matter of urgency, with the DPO consulted on its contents.

- What formal, organisational, practical and technical measures are in place to ensure the security and confidentiality of the data?

  NB: Under Article 23 GDPR, controllers and processors must implement "appropriate technical and organisational measures to ensure a level of security appropriate to the risk[s]" that the processing poses to the rights and freedoms of natural persons (including in particular the data subjects). The article lists various measures such as pseudonymisation

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

and encryption, confidentiality clauses, technical measures to ensure the integrity, availability and resilience of the systems used and restoring capabilities.

The issue will be further addressed in Task 3 (risk assessment). However, an **initial overview** of the measures taken (or not taken) should already be obtained in the context of Task 2, to give a **preliminary indication** of whether the measures taken are "appropriate" in the light of "the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons" (as it is put in Article 23).

Many (though not all) of the measures are covered by recognised international standards, such as those listed below. However, it should be noted that those do not always cover all relevant issues, e.g., they tend to focus on security rather than data minimisation or purpose-limitation.[332]

Even so, **DPOs should be aware of standards** such as these – and **check to see if their DPA or the EDPB has commented on them** (in a positive or negative way, or with additions):[333]

- ISO/IEC 27001:2013 Code of practise for information controls
- ISO/IEC 29100 - Information technology — Security techniques — Privacy framework
- ISO/IEC 27018 - Code of practice for PII protection in public clouds acting as PII processors
- ISO/IEC 29134 - Guidelines for privacy impact assessment (PIA)
- ISO/IEC 29151 - Code of practice for the protection of personally identifiable information
- JIS 15001:2006 - Personal Information Protection Management System requirements
- BS 10012:2017 - Specification for a personal information management system

Further standards are in preparation:

- ISO 20889 - Privacy enhancing data de-identification techniques
- ISO 29184 - Online privacy notices and consent
- ISO 27552 Enhancement to ISO/IEC 27001 for privacy management – Requirements → New title: Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines
- UNI Reference practice – Guidelines on personal data management in ICT environments under GDPR

If a "cloud" is used in the processing, consideration should also be given as to whether the matters have been addressed that are listed in the "Trusted Cloud – Data Protection Profile for Cloud Services (TCDP)" guidelines issued by the German-government-backed pilot project "Data Protection Certification for Cloud Services"

[332] Some years ago, DPAs noticed that an ISO paper on security which covered PIN codes did not specify the number and nature of the characters that should be used. Since then, the DPAs have a policy to interact as much as possible with ISO groups whose activities relate to any DP subject.

[333] Source: Alessandra de Marco, presentation to the first "T4DATA" training session, June 2018, slides on "*Existing standards (on security and privacy)*" and "*Standards (on privacy) not yet finalised*".

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

(although to date those still refer to the German pre-GDPR Federal Data Protection Law, rather than to the GDPR).[334]

At this stage, the DPO should check whether the controller and/or the business owners are aware of the above standards, and are aiming to apply them, and if so, whether there are certifications to that effect. The question of whether they are actually fully complied with, or indeed should be, can be more fully addressed in Task 3 (risk assessment).

This review is the first instance of the DPO's "*(Ongoing Monitoring of compliance*" function (further noted under that heading after Task 4).

If in any respect, it is the DPO's view that a personal data processing operation does not meet any of the GDPR requirements, the DPO must **advise** the relevant internally-responsible person or persons of the deficiencies, and propose remedial action (up to and including stopping the operation altogether if necessary). In case this advice is not followed, the DPO should refer the issue to top management (see below, under "*Advisory tasks*").

Note that this general review of processing operations is a separate issue from the situation of a personal data breach occurring, as discussed in relation to Task 6 ("*Dealing with personal data breaches*"): as explained there, those breaches should be *immediately* reported to highest management.

The DPO should keep full **records** of all her reviews and assessments, and of such advice.

- o – O – o -

[334] See: https://tcdp.de/data/pdf/14_TCDP_v1.0_EN.pdf (see in particular the list of standards on pp. 14 – 16). The version available at the time of writing (v.1.0) dates from September 2016, but the authors hope that – after GDPR-underpinned auditing standards and certification procedures have been created – "*TCDP certifications will be converted into certifications pursuant to the General Data Protection Regulation for cloud services.*" (p. 7). Cf. also the discussion of the risk factors etc., identified by the European Data Protection Supervisor in relation to cloud services, discussed in Task 3, below.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

TASK 3: Assessing the risks posed by the personal data processing operations

As noted at 2.2.1, above, the GDPR imposes a general duty on *controllers* to "[take] into account the nature, scope, context and purposes of processing as well as **the risks of varying likelihood and severity for the rights and freedoms of natural persons**" posed by each personal data processing operation, and to "implement appropriate technical and organisational measuresto ensure and to be able to demonstrate that processing is performed in accordance with this Regulation" (Art. 24(1); cf. also Art. 25(1))).

The DPO, too:

> shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.
>
> (Art. 39(2))

Compliance with these requirements demand that the relevant risks be ascertained. This should be done in connection with the carrying out of the inventory of personal data processing operations and the creation of the register of those operations (Task 1) and, especially, with the review of those operations (Task 2).

The GDPR does not expressly require the involvement of the DPO in any general risk assessments: it stipulates such involvement only in relation to the more in-depth Data Protection Impact Assessments (Art. 35(2) – see Task 4, below). However, in practice it would be highly advisable (to say the least) to involve the DPO also in these more general risk assessments. Indeed, in practice, the assessment will often depend on the views of the DPO.

It should be noted that the risks to be assessed are not just the security risks in a narrow sense – i.e., the likelihood and impact of a **data breach**[335] – but rather, the risks to the **rights and freedoms of the data subjects (and other individuals)** that may be posed by the processing operation. This includes not only their general rights to privacy and private life as well as their specific data subject rights, but also, depending on the case, their rights to freedom of expression, freedom of movement, freedom from non-discrimination, freedom from authoritarian power and the right to stay in a democratic society without undue surveillance by their own, or by other countries, and the right to an effective remedy. The concept is broad.[336]

The general risk assessment should also take into account the findings in Task 2. For instance, if it is found that although a particular processing operation was, as such, lawful (i.e., had a proper legal basis and served a legitimate interest), but that irrelevant and excessive data were collected and held for the relevant purpose, contrary to the "data minimisation" principle – then that can be said to pose a "risk" in itself, i.e., that the irrelevant and unnecessary data would wrongly be used. In such a case, the appropriate measure to avoid that risk would be to stop collecting the irrelevant and unnecessary data,

---

335 A "**personaldata breach**" is defined in the GDPR as: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." (Art. 4(12)). See Task 6, below.

336 Cf. the discussions of the meaning of "risk" and "high risk" in, respectively, Task 1 (under the heading "*Exemptions*") and Task 4.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

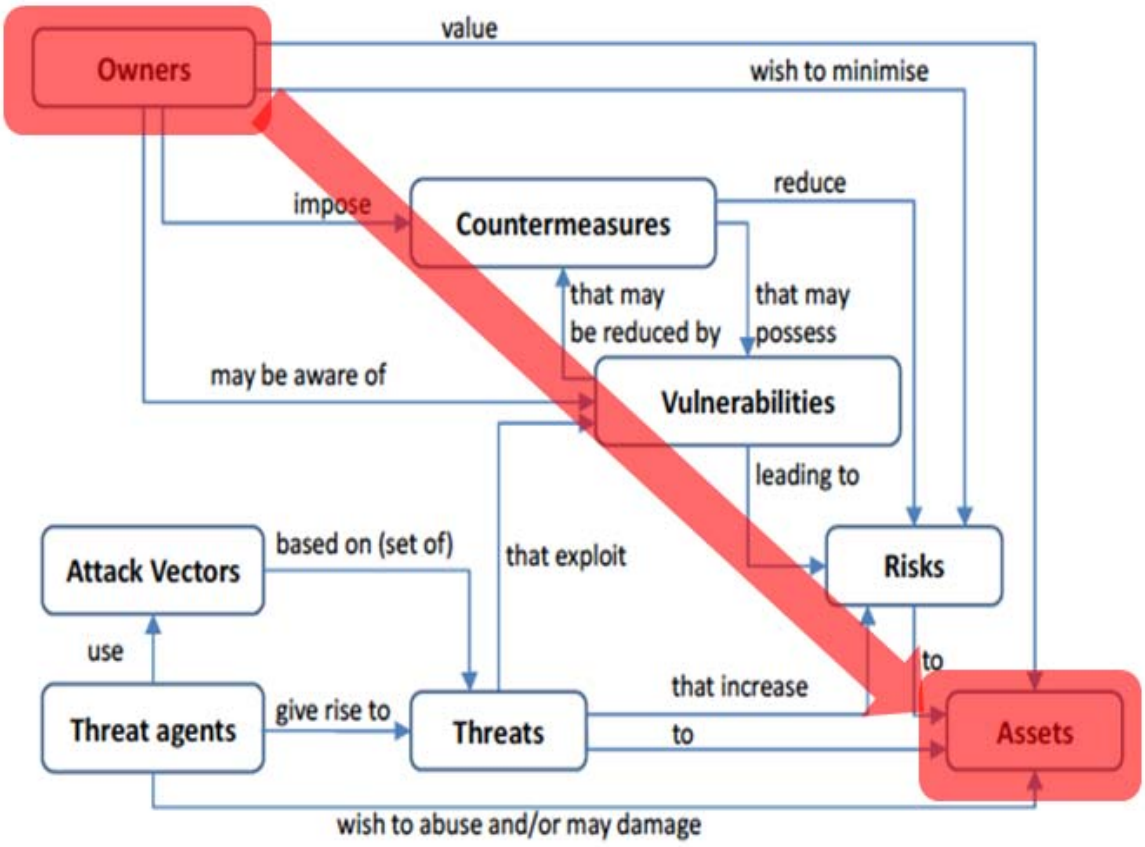
and to erase any such data already held. Another example would be the use of still-identifiable data in statistical processing that can be carried out by means of pseudonymised or even fully-anonymised data – in that case, the appropriate measure would be to ensure that the data used would be properly (seriously) pseudonymised or (preferably) full anonymised.

All this underlines that for the general review (Task 2) and the risk assessment (the present Task 3), the controller – in practice, the DPO – must look closely at **all aspects** of **each distinct personal data processing operation and -function**.

As proposed by the Italian data protection authority, the *Garante*, it is useful to follow the approach adopted by ENISA (the EU Agency for Network and Information Security), which in turn builds on the widely accepted standard ISO 27005: "*Threats abuse vulnerabilities of assets to generate harm for the organisation*"; and to consider in more detailed terms **risk** as being composed of the following ***elements***:

Asset (Vulnerabilities, Controls), **Threat** (Threat Agent Profile, Likelihood) and **Impact**.

The elements of risk and their relationships can then be illustrated as follows:



Source: ENISA Threat Landscape Report 2016, Figure 4: The elements of risk and their relationships according to ISO 15408:2005, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016. See also its 2017 report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

As also outlined by the *Garante*, **a proper risk assessment involves four steps**:[337]

1. Definition of the processing operation and its context.
2. Understanding and evaluation of impact.
3. Definition of possible threats and evaluation of their likelihood (threat occurrence probability).
4. Evaluation of risk (combining threat occurrence probability and impact).

The first (defining the processing operation and its context) were done in Tasks 1 and 2, above.

The second step involves **defining different levels of impact** – which can sensibly be left at four levels, as follows:[338]

LEVEL of impact	Description
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
Very high	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

The *Garante* notes **four main assessment areas** in terms of **data security**, i.e.:

A. Network and technical resources (hardware equipment and software)
B. Processes/procedures related to the data processing operation
C. Different parties and people involved in the processing operation
D. Business sector and scale of the processing

For each assessment area, it asks **five questions**, a positive answer to which indicates a risk, as set out in the table, overleaf.[339]

337 Giuseppe d'Acquisto, presentation to the first "T4DATA" training session on data security, June 2018, slide on "*Risk assessment (a focus on security)*".
338 *Idem*, slide on "*Understanding and evaluating impact*".
339 *Idem*, slides on each of these four main assessment areas, with further explanation as to why a positive answer to the question in each case poses a security risk.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

The person assessing the security risk can, from these answers, then calculate the **threat occurrence probability**, as indicated in the two charts under that heading, after the table, overleaf.This score can then be combined with the impact score to arrive at an **overall risk score**, as indicated in the chart after those.

THE FOUR MAIN ASSESSMENT AREAS IN TERMS OF DATA SECURITY:

A. Network & technical resources:	B. Processes & procedures	C. Parties & people involved	D. Business sector & scale
1. Is any part of the processing of personal data performed through the internet?	**6.** Are the roles and responsibilities with regard to personal data processing vague or not clearly defined?	**11.** Is the processing of personal data performed by a non-defined number of employees?	**16.** Do you consider your business sector as being prone to cyberattacks?
2. Is it possible to provide access to an internal personal data processing system through the internet (e.g. for certain users or groups of users)?	**7.** Is the acceptable use of the network, system and physical resources within the organization ambiguous or not clearly defined	**12.** Is any part of the data processing operation performed by a contractor/third party (data processor)?	**17.** Has your organization suffered any cyberattack or other type of security breach over the last two years?
3. Is the personal data processing system interconnected to another external or internal (to your organization) IT system or service?	**8.** Are the employees allowed to bring and use their own devices to connect to the personal data processing system?	**13.** Are the obligations of the parties/persons involved in personal data processing ambiguous or not clearly stated?	**18.** Have you received any notifications and/or complaints with regard to the security of the IT system (used for the processing of personal data) over the last year?
4. Can unauthorized individuals easily access the data processing environment?	**9.** Are employees allowed to transfer, store or otherwise process personal data outside the premises of the organization?	**14.** Is personnel involved in the processing of personal data unfamiliar with information security matters?	**19.** Does a processing operation concern a large volume of individuals and/or personal data?
5. Is the personal data processing system designed, implemented or maintained without following relevant best practices?	**10.** Can personal data processing activities be carried out without log files being created?	**15.** Do persons/ parties involved in the data processing operation neglect to securely store and/or destroy personal data?	**20.** Are there any security best practices specific to your business sector that have not been adequately followed?

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

THREAT OCCURANCE PROBABILITY (1):

Assessment area:	Nr of "yes" answers	Level	Score
A. Network & technical resources:	0 – 1	Low	**1**
	2 – 3	Medium	**2**
	4 – 5	High	**3**
B. Processes & procedures	0 – 1	Low	**1**
	2 – 3	Medium	**2**
	4 – 5	High	**3**
C. Parties & people involved	0 – 1	Low	**1**
	2 – 3	Medium	**2**
	4 – 5	High	**3**
D. Business sector & scale	0 – 1	Low	**1**
	2 – 3	Medium	**2**
	4 – 5	High	**3**

The above scores can then be entered into the following summary chart:

THREAT OCCURANCE PROBABILITY (2):

Overall SUM of scores:	Threat occurrence PROBABILITY LEVEL:
4 – 5	**Low**
6 – 8	**Medium**
9 – 12	**High**

Finally, these results can then be combined with the "Impact Level" results set out in the first chart, above, to indicate the overall risk, as follows:

OVERALL RISK ASSESSMENT:

		IMPACT LEVEL		
		Low	**Medium**	**High/Very High**
THREAT OCCURANCE PROBABILITY	**Low**			
	Medium			
	High			

Legend:

[ ] *Low risk* [ ] *Medium risk* [ ] *High risk*

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

NOTE HOWEVER that the above risk assessment scheme relates mainly to **data security risks.**

That is certainly one major category of risk that is to be assessed and addressed – and not just once, but on a continual basis, as risks can evolve and mutate over time. Cf. the Note headed: "*Monitoring of compliance: Repeating Tasks 1 – 3 (and 4) on an ongoing basis*" at the end of the discussion of Task 4, just before the discussion of Task 5, below.

However, the GDPR also, more generally, refers to "**risk[s] to the rights and freedoms of natural persons**" (see Articles 34, 35 and 36). The first article, Article 34, clearly accepts that data breaches, as such, can result in such risks, and imposes important rules on how to deal with them, as discussed in Tasks 4 (DPIAs), 5 (Investigation Task), 10 (Cooperation with the DPA) and 12 (Information and Awareness-Raising Task).

However, it should be noted that **"risks to the rights and freedoms of natural persons" do not flow only from data breaches**. The GDPR itself stipulates in Article 35(1) that "*high* risks" of this kind can stem, in particular, from:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10;

  or
- a systematic monitoring of a publicly accessible area on a large scale.

In these cases, *preciselybecause such processing operations pose **inherently high risks** to the rights and freedoms of individuals*, a Data Protection Impact Assessment is required (and in some cases the relevant DPA or DPAs must be consulted), as discussed in the next task.

More specifically, profile-based automated decision-making can lead to **unfair decisions** (because no one is completely the same as any other individual, and no system would, hopefully, know everything about a person) or undemocratic decisions with **discriminatory yet unchallengeable outcomes**;[340] the use of sensitive data can also lead to **discrimination** (whether intentional or not);[341] the use of even seemingly innocuous sales data can reveal intimate health issues or pregnancy);[342] and systematic monitoring of people in public places can have a **chilling effect on the exercise of fundamental rights such as the rights to**

[340] See: Douwe Korff & Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, report prepared for the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) of the Council of Europe, 2015, section I.iii, *The dangers inherent in data mining and profiling*, available at: https://rm.coe.int/16806a601b

[341] Which is why special, especially restrictive, rules on the processing of personal data were included in the European data protection instruments: see the "NB" in Part One, section 1.2.3, on p. 17, above.

[342] See: *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, Forbes, 16 February 2012, available at: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#2ea04af16668

freedom of expression, association and protest.[343] Indeed, the risks can be combined and then become **mutually reinforcing**, as in the use of face recognition technology in the monitoring of public places by the police, with the aim of "identifying" bad people and predicting bad behaviour.[344]

Note that for these risks to materialise, no data breach is required: the risks stem from the inherently dangerous features of the processing operations themselves, even if performed in accordance with their specifications and without a data breach as defined in the GDPR. ***That is not captured by the (otherwise very useful) risk assessment scheme outlined by the* Garante*, reproduced above.***

The same is true as concerns lesser "risks to the rights and freedoms of natural persons", stemming from processing operations, not listed as inherently posing a "high risk". This includes in particular processing operations that do not fully meet the requirements of the GDPR.

EXAMPLES:

- Using personal data collected for one purpose for another, not "compatible" purpose without a proper legal basis for the secondary processing and/or without adequately informing the data subjects of the intended secondary uses of their data – which would be made worse if this involves a disclosure of the data to a third party.

➢ This can result in the data subjects being denied the opportunity to consent (or not consent, or object) to the secondary processing, which may affect them in a negative way (e.g., in job or credit applications). It is also quite likely that personal data obtained in one context are not sufficiently accurate or relevant for use in an entirely different context.

- Retaining and/or using personal data (typically, once they are no longer needed for their original purpose) in pseudonymised or supposedly anonymised form (typically, for further use in this form for a new, secondary purpose).

➢ In view of the increasing risk of re-identification of even supposedly fully-anonymised data,[345] any such retention and use of pseudonymised or supposedly anonymised data must be regarded as posing risks to the rights and freedoms of the data subjects (which may even amount to likely "high risks", requiring a Data Protection Impact Assessment, as discussed in Task 4). The DPO should most carefully check the risks of re-identification of such data in any

[343] See the quote from the famous *Census* judgment of the German Constitutional Court on p. 10 of this handbook.

[344] See: Douwe Korff, *First Do No Harm: The potential of harm being caused to fundamental rights and freedoms by state cybersecurity interventions*, section 2.4, *Preventive, predictive policing*, in: Ben Wagner, Matthias C. Kettemann and Kilian Vieth (Eds.), Research Handbook on Human Rights & Digital Technology: Global Politics, Law & International Relations, Centre for Internet and Human Rights, Berlin, due for publication later in 2018,

[345] For an easy-to-read summary of the issues with de- and re-identification, see the submission by the Foundation for Information Policy Research to the UK Government consultation on Making Open Data Real, October 2011, available at: www.fipr.org/111027opendata.pdf. This refers to the seminal paper on the problem: Paul Ohm, Broken promises of privacy: responding to the surprising failure of anonymization, 57 UCLA Law Review (2010) 1701, available at: http://papers.ssrn.com/sol3/paperscfm?abstract_id=1450006.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

specific uses, and impose strong mitigating factors (such as "differential privacy")[346] in appropriate cases – or refuse to allow the further processing of the data.

- Using irrelevant, incorrect or out-dated information – with possible similar negative consequences.

- Not giving appropriate weight to "the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child", when assessing whether personal data can be processed on the basis of the "legitimate interest" condition (Art. 6(1)(f) GDPR).

➢ This by definition causes harm to those data subject interests. The use of the "legitimate interest" criterion as a legal basis for processing therefore always requires particularly close scrutiny by the DPO in the present task.

➢ **NB:** The criterion cannot be relied upon by public authorities "in the performance of their tasks" (Art. 6(1), final sentence), but this does not mean that the question never arises in a public sector context, e.g., in relation to not-statutorily-required tasks such as emailing citizens about cultural events, using the population register; or in relation to activities by private entities carrying out tasks "in the public interest".

- Not properly informing data subjects of all of the many details of which they must be informed under Articles 13 and 14 GDPR.

➢ This can result in the data subjects not being able to fully exercise their rights under the GDPR (which are of course precisely the kinds of "interests or fundamental rights and freedoms of the data subject which require protection of personal data" to be protected).

- Transferring personal data to a third country that has not been held to provide "adequate" protection to personal data, without having appropriate safeguards or a set of approved Binding Corporate Rules (BCRs) in place, or without otherwise relying on one of the specified derogations (cf. Article 46 – 48 GDPR). This includes using a "cloud" service that uses a server (or servers) that are in such third countries.

➢ As the EDPS has pointed out in his detailed advice on the use of cloud services by the EU institutions (which should also be studied by national public bodies as much of the advice could be equally applied to them), cloud computing poses specific risks that should be most carefully addressed by controllers (relying on their DPOs).347 Indeed, his advice suggests that cloud computing may well have to be regarded as inherently posing high risks and therefore requiring a Data Protection Impact Assessment. This is noted in the next task.

- Outsourcing the processing of personal data by public authorities, in particular if the data are sensitive in the technical-legal sense of the GDPR ("special categories of

---

346 Differential privacy is an important measure to prevent re-identification of data subjects from datasets – but it only works if applied in a controlled environment, in which researchers are limited in the queries they can send to the database, see:
https://privacytools.seas.harvard.edu/differential-privacy
https://people.eecs.berkeley.edu/~stephentu/writeups/6885-lec20-b.pdf
It does not provide an answer to circumstances in which personal data are released in supposedly fully-anonymised form to the general public, or in which large datasets are otherwise matched without full control.

347 European Data Protection Supervisor (EDPS), Guidelines on the use of cloud computing services by the European institutions and bodies, March 2018, available at:
https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf
See in particular *Annex 4: Data protection-specific risks of cloud computing*

data" – Article 9), or sensitive in more general terms, such as financial data or census data.

- The EDPS notes that the use of cloud computing aggravates the risks inherent in outsourcing of processing.[348]

If, after the assessment has been carried out, it is the DPO's view that a personal data processing operation does pose a risk to relevant interests, the DPO must **advise** the relevant internally responsible person or persons of those risks, and propose **mitigating or alternative action**. Often, a legitimate purpose can be achieved by different, less intrusive means, or by the use of less (and less sensitive) data – and in such cases, the DPO should forcefully suggest that. In case this advice is not followed, the DPO should again **refer** the issue to top management (see further under "*Advisory tasks*").

Again, the DPO should keep full **records** of all these risk assessments, and of such advice.

If the DPO's advice is followed, these records will "**demonstrate** that processing is performed in accordance with this Regulation" – i.e., that those risks have indeed been assessed and that the measures taken in the light of that assessment were appropriate to those risks (Cf. Art. 24(1) and the discussion of the "duty to demonstrate compliance" with the GDPR in section 2.2, above).

Note that if the general risk assessment indicates that a proposed processing poses a likely "**high risk**" to the rights and freedoms of individuals, the DPO should advise the controller that a full Data Protection Impact Assessment (DPIA) is required, as discussed next, in Task 4.

Note that, even if a DPIA is not required, the DPO will have to continue to monitor all her controller's personal data processing operation on an ongoing basis: see the discussion after Task 4, under the heading "*Monitoring of compliance: Repeating Tasks 1 – 3 (and 4) on an on going basis"*.

Note also that often national legislators will already have tried to address special risks which they believe are posed by special processing operations or activities, in their national rules – something which to a large extent can be continued under the "specification clauses" in the GDPR.[349]

Examples:

In **Croatia**, processing of ***genetic data*** for the calculation of the risk of disease and other health aspects of data subjects in relation to the conclusion or execution of life insurance contracts and contracts with clauses on survival is prohibited - and this prohibition cannot be lifted by the consent of the data subject (Art. 20 of the Law implementing the GDPR).

There, and in other countries, the use of ***biometric data*** and ***closed-circuit television (CCTV) surveillance cameras*** is also subject to special conditions, such as a requirement of especially clear and unambiguous consent, and constraints, such as the placing of limits on data retention.

---

348 The EDPS Guidelines on the use of cloud computing services by the European institutions and bodies (previous footnote) "focuses on the use of cloud computing services provided by commercial entities [but] [a]s such it also addresses, as a natural consequence, the issues raised by the outsourcing of IT services that process personal data." (p. 5).

349 See Part Two, section 2.2.

Such legal conditions should of course also be fully taken into account in any risk assessment: no controller or DPO could of course ever conclude that a risk was acceptable even though the special legislative conditions and constraints were not met.

- o – O – o -

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

TASK 4 Dealing with operations that are likely to result in a "high risk": carrying out a Data Protection Impact Assessment (DPIA)

What was said above about general risk assessments (Task 3) applies *a fortiori* to personal data processing operations which, on the basis of the above general risk assessment, are held to pose alikely "**high risk** to the rights and freedoms of natural persons" (Art. 35(1)). The GDPR makes clear that this may in particular be the case when "new technologies" are used.

If the preliminary risk assessment carried out in Task 3 does indeed indicate that a particular personal data processing operation poses such a likely "high risk", then the controller is required to carry out a **Data Protection Impact Assessment** (DPIA) before going ahead with the operation.

The GDPR stipulates that a DPIA must in any case take place in cases of fully-automated/profile-based decision-making, large-scale processing of sensitive data, or large-scale monitoring of a publicly accessible area (Art. 35(3)). National DPAs must also adopt lists of operations that will be subject to DPIAs in their territory, and may adopt lists of operations that will not require one – but these lists have to be submitted to the EDPB, and can be challenged by other DPAs under the GDPR's "consistency mechanism" (Art. 35(4) – (6)). The GDPR also allows the EDPB to issue a negative and positive list of its own, drawing on the ones submitted to it by the national DPAs (who are required to do so under Article 64(1)(a) GDPR).

In practice, what has happened was that, first of all, the Article 29 Working Party issued extensive advice and guidelines on the carrying out of a DPIA, both in its Guidelines on DPOs of December 2016, as revised in April 2017 (WP243 rev1)[350] and in its later, more elaborate Guidelines on DPIAs, adopted on 4 April 2017, as revised and adopted on 4 October 2017 (i.e., all still before the GDPR applied).[351] Both were endorsed by the European Data Protection Board on the day the GDPR came into full application, 25 May 2018.[352]The EDPS also provided useful further guidance in his paper on Accountability on the ground[353] including a provisional list of processing operations that, in his view, do or do not require a DPIA.[354]

The Revised Guidelines on DPIAs, adopted by the WP29 and endorsed by the EDPB, set out **nine criteria** that should be taken into account in determining whether a processing operation is likely to result in a "high risk", and say that:[355]

> ***In most cases***, a data controller can consider that a processing meeting **two criteria** would require a DPIA to be carried out. In general, the WP29 considers that the more criteria are met by the processing, the more likely it is to present a high risk to the

[350] See footnote 242, above.

[351] WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248 rev 1, hereafter referred to as the WP29 Guidelines on DPIAs), contents page, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[352] See footnote 248, above.

[353] EDPS, Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments (footnote 302, above), section 4, *When to carry out a DPIA?*, at pp. 9 – 11.

[354] *Idem*, Annex 5.

[355] WP29 Guidelines on DPIAs (footnote 351, above), p. 11, emphases added.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

> rights and freedoms of data subjects, and therefore to require a DPIA, regardless of the measures which the controller envisages to adopt.

This is further discussed below, under the heading "*How to assess whether a proposed processing operation is likely to result in a 'high risk'*", where examples are provided taken from the WP29 Guidelines and the EDPS paper, under the sub-heading "*Factors that indicate 'high risks'*".

Here, we should note that, next, mostof the national DPAs (22 out of the 28)[356] adopted their own provisional lists, and submitted those to the EDPB for review. The EDPB carried out those reviews in the light of the WP29 Guidelinesit had endorsed and on 25 September 2018 issued 22 opinions on those lists (one on each draft list).[357] The main point consistently made by the EDPB in these opinions was a recommendation to the DPAs that they should not include processing operations in the list of operations for which a DPIA is mandatory, if the operation in question met only *one* of the criteria for determining whether there was a likely "high risk", set out in the Guidelines. Thus, for instance, in its opinion on the draft list submitted by the United Kingdom, it says:[358]

> The list submitted by the Supervisory Authority of the United Kingdom for an opinion of the Board states, that the processing of biometric data falls under the obligation to perform a DPIA on its own. The Board is of the opinion that the processing of biometric data on its own is not necessarily likely to represent a high risk. However, the processing of biometric data for the purpose of uniquely identifying a natural person in conjunction with at least one other criterion requires a DPIA to be carried out. As such, the Board requests the Supervisory Authority of the United Kingdom to amend its list accordingly, by adding that the item referencing the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction of at least one other criterion, to be applied without prejudice to article 35(3) GDPR.

But of course, a DPIA may be carried out by a controller even if only one of those criteria is met, without this being an obligation.

The requirement for a DPIA can be obviated in cases in which a law regulates the kind of operation in question and a general DPIA has been carried out in the context of the adoption of the law (Art. 35(10)). Furthermore, "[a] single [DPIA] assessment may address a set of similar processing operations that present similar high risks" (Art. 35(1), last sentence). As the WP29 summed it up:[359]

> When isn't a DPIA required? When the processing is not "likely to result in a high risk", or a similar DPIA exists, or it has been authorized prior to May 2018, or it has a legal basis, or it is in the list of processing operations for which a DPIA is not required.

---

[356] Austria, Belgium, Bulgaria, Czech Republic, Germany, Estonia, Greece, Finland, France, Hungary, Ireland, Italy, Lithuania, Latvia, Malta, the Netherlands, Poland, Portugal, Romania, Sweden, Slovakia and the United Kingdom.

[357] All are available through links provided at:
https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en

[358] EDPB, Opinion 22/2018 on the draft list of the competent supervisory authority of the United Kingdom regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR), adopted on 25 September 2018, available at:
https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_uk_sas_dpia_list_en.pdf

[359] WP29 Guidelines on DPIAs (footnote 351, above), contents page, p. 6.

Extensive guidance on DPIAs, including methodological guidance, has also been issued by national DPAs, including those of France, Spain and the UK, and by the German *Datenschutzzentrum* (endorsed by the German DPAs).[360] The **French** data protection authority, the CNIL, has even (in cooperation with other DPAs) developed an open-source DPIA software tool that "aims to help data controllers build and demonstrate compliance to the GDPR". As explained on the website:[361]

> **Who can use the PIA software?**
>
> The tool is mainly addressed to data controllers who are slightly familiar with the PIA process. In this regard, a stand-alone version can be downloaded and easily launched on your computer.
>
> It is also possible to use the tool on an organisation's servers in order to integrate it with other tools and systems already used in-house.
>
> **What is it?**
>
> The PIA tool has been designed around three principles:
>
> - **A didactic interface to carry out PIAs:** the tool relies on a user-friendly interface to allow for a simple management of your PIAs. It clearly unfolds the privacy impact assessment methodology step by step. Several visualisation tools offer ways to quickly understand the risks.
> - **A legal and technical knowledge base:** the tool includes the legal points ensuring the lawfulness of processing and the rights of the data subjects. It also has a contextual knowledge base, available along all the steps of the PIA, adapting the contents displayed. The data are extracted from the GDPR, the PIA guides and the Security Guide from the CNIL, to the aspect of the processing studied.
> - **A modular tool:** designed to help you build your compliance, you can customise the tool contents to your specific needs or business sector, for example by creating a PIA model that you can duplicate and use for a set of similar processing operations. Published under a free licence, it is possible to modify the source code of the tool in order to add features or include it into tools used in your organisation.

There is no space in this handbook to cover all the detailed advice on DPIAs provided for in the later, more specific WP29 (EDPB-endorsed) guidance on DPIAs, or in the national guidance: **the reader is strongly encouraged to study the WP29/EDPB guidance in full, and**

---

[360] See the list with links in *Annex 1* to the WP29 Guidelines on DPIAs (footnote 351, above). The methodologies for DPIAs are further discussed below, under that heading.

[361] Available, with further information in English, at:
https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
The CNIL uses the shorter acronym "PIA" (also in the quoted text, above), presumably because DPIAs originate from "*Privacy* Impact Assessments". Note that the tool has been recently updated. Information on the update is available here (in French only):
https://www.cnil.fr/fr/loutil-pia-mis-jour-pour-accompagner-lentree-en-application-du-rgpd
On that page, the CNIL says the software is available in 14 languages: French, English, Italian, German, Polish, Hungarian, Finnish, Norwegian, Spanish, Czech, Dutch, Portuguese, Romanian and Greece, and that it has been endorsed (at least provisionally, in the beta version) by the data protection authorities of Bavaria, Italy, Finland, Hungary, Poland and Norway. Note however that the software is mainly focused on technical security, and will be mainly of use to SMEs, rather than to large and very complex entities.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

relevant national advice where relevant, and rely on it in their actions and any advice given.[362]

The reader, and especially DPOs, should also take account of the national mandatory DPIA list published by their respective DPA as that list contains examples of situations where application of the above guidance and advice has resulted into prescribing the performance of a DPIA by both public and private entities; DPOs are expected to supervise the carrying out of a DPIA by the respective controllers whenever they are mandated to do so based on the said lists. If "white lists" are also issued in the next months (under Article 35(5) GDPR), these will also be quite helpful as they will rule out the need for the controller to engage in this exercise for a set of non-high risk processing activities.

Below, we will briefly note the guidance in relation to: **the different roles and responsibilities of the controller and the DPO**; the question of **how to assess whether a proposed processing operation is likely to result in a "high risk"**; the **methodologies for DPIAs**, and **what to do with the record of the DPIA**, in particular if it is concluded that certain identified high risks cannot be fully mitigated by various possible measures, in which case the GDPR requires that **the relevant DPA be consulted** (Art. 36).

The different roles and responsibilities of the controller and the DPO in relation to DPIAs

In its Guidelines on DPOs, the WP29 again stressed the distinct roles and responsibilities of the controller and the DPO, also in relation to DPIAs. It wrote:[363]

> 4.2. The DPO's role in a data protection impact assessment
>
> According to Article 35(1), it is the task of the controller, not of the DPO, to carry out, when necessary, a data protection impact assessment ('DPIA'). However, the DPO can play a very important and useful role in assisting the controller. Following the principle of data protection by design, Article 35(2) specifically requires that the controller '*shall seek advice*' of the DPO when carrying out a DPIA. Article 39(1)(c), in turn, tasks the DPO with the duty to '*provide advice where requested as regards the [DPIA] and monitor its performance*'.
>
> The WP29 recommends that the controller should seek the advice of the DPO, on the following issues, amongst others:[364]
>
> - whether or not to carry out a DPIA
> - what methodology to follow when carrying out a DPIA
> - whether to carry out the DPIA in-house or whether to outsource it
> - what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects

[362] See the references in footnotes 249, 318, 351 and 353 and in the previous footnote, above, for the main advice to be studied.

[363] WP29 Guidelines on DPOs (footnote 242, above), section 4.2, pp. 16 – 17, original italics, underlining in the last paragraph added.

[364] Article 39(1) mentions the tasks of the DPO and indicates that the DPO shall have 'at least' the following tasks. Therefore, nothing prevents the controller from assigning the DPO other tasks than those explicitly mentioned in Article 39(1), or specifying those tasks in more detail. [original footnote]

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

- whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR

If the controller disagrees with the advice provided by the DPO, the DPIA documentation should specifically justify in writing why the advice has not been taken into account.[365]

The WP29 further recommends that the controller clearly outline, for example in the DPO's contract, but also in information provided to employees, management (and other stakeholders, where relevant), the precise tasks of the DPO and their scope, in particular with respect to carrying out the DPIA.

The later WP29 Guidelines on DPIAs also stress that DPIAs are to be carried out by "[t]he controller, with the DPO and processors".[366]

In practice, especially in smaller organisations, the DPO will often again play a (if not indeed the*) leading part in the assessment.*

How to assess whether a proposed processing operation is likely to result in a "high risk"

The WP29/EDPB explain that:[367]

> The obligation for controllers to conduct a DPIA in certain circumstances should be understood against the background of their general obligation to appropriately manage risks presented by the processing of personal data –

i.e., as also noted above, the question of whether a DPIA should be carried out arises naturally from the general duty of the controller – carried out with the "advice", but in practice generally in reliance on, the DPO – to assess the risks inherent in all the controller's personal data processing operations (Task 3, above).

They go on to clarify the concept of "risk" and the protected interests that should be taken into account:[368]

> A "risk" is a scenario describing an event and its consequences, estimated in terms of severity and likelihood. "Risk management", on the other hand, can be defined as the coordinated activities to direct and control an organization with regard to risk.
>
> Article 35 refers to a likely high risk "to the rights and freedoms of individuals". As indicated in the Article 29 Data Protection Working Party Statement on the role of a risk-based approach in data protection legal frameworks, the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech,

---

365 Article 24(1) provides that '*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary*'. [original footnote, original italics]

366 See WP29 Guidelines on DPIAs (footnote 351, above), section III.D.b).

367 *Idem*, p. 6.

368 *Idem*. Note also the reference earlier to ISO 31000:2009*, Risk management — Principles and guidelines*, International Organization for Standardization (ISO) ; ISO/IEC 29134 (project), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, International Organization for Standardization (ISO) (WP29 Guidelines on DPIAs, footnote 351, on p. 5).

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

> freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

The WP29 notes the examples in Article 35(3) of the GDPR of situations that inherently pose "high risks", already mentioned: when a controller uses automated, profile-based algorithms to take decisions with legal or other significant effect; when the controller processes sensitive data or data on criminal convictions "on a large scale"; or when the controller "systematically monitors" a publicly-accessible area "on a large scale". It the rightly adds:[369]

> As the words "in particular" in the introductory sentence of Article 35(3) GDPR indicate, this is meant as a non-exhaustive list. There may be "high risk" processing operations that are not captured by this list, but yet pose similarly high risks. Those processing operations should also be subject to DPIAs.

The WP29 lists a number of factors – most but not all related to the three examples in Article 35 – that suggest that a processing operation poses "high risks", and gives further, more specific examples. The EDPS provides further examples, both in his provisional list of processing operations that will always require a DPIA, and in a template that can be used to assess whether processing operations that figure neither in his "positive" list (operations that in his view always require a DPIA) nor in his "negative" one (those that in his view do not require a DPIA) should be subjected to a DPIA.[370] These WP29 and EDPS examples are set out below (somewhat redacted, with the WP29 examples removed from the text and moved to the box, and the EDPS examples indicated by an *). We have added some further examples (or further details or variations), of relevance to public-sector controllers in particular; those examples etc. are set out in *italics*.

Factors that indicate "high risks"[371]

1. Evaluation or scoring, including profiling and predicting, especially from "*aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements*" (recitals 71 and 91).

> **Examples:**
>
> A financial institution that screens its customers against a credit reference database or against an anti-money laundering and counter-terrorist financing (AML/CTF) or fraud database.
>
> A bank screening transactions in accordance with applicable law to detect possibly fraudulent transactions.*
>
> Profiling staff members based on all their transactions in [*the organisation's*] case management system with automatic reassignment of tasks.*

369 *Idem*, p. 9.

370 The positive and negative lists are set out in *Annex 5* to the EDPS Accountability on the ground paper (footnote 353, above); the *Template for threshold assessment/criteria* is contained in *Annex 6* of that paper.

371 As listed and numbered in WP29 Guidelines on DPIAs (footnote 351, above), pp. 9 – 10. The main comments in relation to the factors are also taken from those guidelines. Note that the factors somewhat overlap, or can be combined, as is noted under the factors under the heading "*Multi-factor high-risk operations*".

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

A biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks.

A company building behavioural or marketing profiles based on usage or navigation on its website.

2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person" (Article 35(3)(a)), in particular (but not only) in cases in which the processing may lead to the exclusion or discrimination against individuals.

Examples:[372]

Automated staff appraisal ("if you're in the lowest 10% of the team for the number of cases dealt with, you'll receive a 'unsatisfactory' in your appraisal, without discussion").*

Identification of "possible" or "probable" tax fraudsters by means of the automatic attribution of profiles to taxpayers.[373]

Identification of "possible" or "probable" welfare fraudsters on the basis of a profile of known fraudsters.

Identification of children "at risk" of growing up to becoming obese or gang members or criminals, or of girls "likely" to become pregnant in their teens, on the basis of profiles.[374]

Identification of young people and adults as "at risk" of being "radicalised".

3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or "*a systematic monitoring of a publicly accessible area*" (Article 35(3)(c))15. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s).

---

[372] The WP29/EDPB adds that "*Processing with little or no effect on individuals does not match this specific criterion. Further explanations on these notions will be provided in the upcoming WP29 Guidelines on Profiling*." (p. 9).

[373] Such attributions were made in **Italy** by the Italian Revenue Agency, using a tool called *Redditometro*. The profiles were based, amongst others, on assumed expenses made by taxpayers deduced, according to statistical parameters, from their allocation in specific family categories or geographical areas. This profiling tool was investigated by the Italian DPA, the *Garante*. One of the main issues was the low quality of the data and the resulting high error rate based on unreliable inferences drawn from the data. On the basis of its investigation, the *Garante* prescribed that a taxpayer's real income could only be calculated from actual, documented expenses, and not deduced from statistically-based assumptions of levels of expenses. See: https://www.garanteprivacy.it/en/home/docweb/-/docweb-display/docweb/2765110

[374] See the UK Foundation for Information Policy (FIPR), Childrens Databases - Safety & Privacy, study for the UK Information Commissioner, 2006, available at: https://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf

Examples:

Internet traffic analysis breaking encryption.*

Covert CCTV.*

Smart CCTV [*e.g., using face-recognition software*] in publicly accessible spaces.*

Data loss prevention tools breaking SSL encryption.*

Processing of metadata (e.g. time, nature and duration of a bank account transaction) for organisational purposes or to provide budgetary estimates.[375]

4. Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, health-, genetic- or biometric data, and data on sexual orientation*), as well as personal data relating to criminal convictions or offences as defined in Article 10. Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (*see the third example, below*), or because they impact the exercise of a fundamental right (*see the fourth example*) or because their violation clearly involves serious impacts in the data subject's daily life (*see the fifth example*). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment, [*taking into account whether the data subject could reasonable expect that the data might be used by other people for certain purposes: see the seventh example, below*].

Examples:

A general hospital [*or a welfare office*] keeping patients' [*or welfare claimants'*] medical records.

A private investigator keeping details of criminal convictions or offences, [*or a public authority such as a state educational institution keeping such data in relation to pupils or students at such institutions*].

[*A public body or a private entity (such as an employer)*] accessing personal documents, emails, diaries or notes from e-readers equipped with note-taking features, owned by staff members [*or used by staff for both personal and professional purposes, as in "Bring Your Own Device [BYOD] situations*].

[*A public body or a private entity (such as an employer)*] accessing very personal information contained in life-logging applications, *or using social media information in contexts that can have significant impact on the individuals concerned, such as selection people for jobs (or indeed interviews)*.

Pre-recruitment medical exams and criminal records checks.*

Administrative investigations & disciplinary proceedings.*

375 This example is taken from the **Italian** DPIA list approved by the EDPB.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Any use of 1:n biometric identification.*

Photos used with facial recognition software or used to infer other sensitive data [*e.g., when they can lead to discrimination in a recruitment context*].*

5. Data processed on a large scale: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance.[376] In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

   a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;

   b. the volume of data and/or the range of different data items being processed;

   c. the duration, or permanence, of the data processing activity;

   d. the geographical extent of the processing activity.

Example:

[National- but possibly EU-linked] databases on disease surveillance.*

Large-scale exchanges of data among public sector controllers (e.g. Ministries, local and regional authorities, etc.) via electronic networks.[377]

The large-scale collection of genealogical information on families of people belonging to a particular religious group.[378]

The creation of very large "lifestyle databases" for marketing purposes (but which may – or at least can – also be used for other purposes).

The recording by political parties of the perceived voting intentions of very large numbers of voters (or households) nation- or countrywide, on the basis of doorstep interviews, and the subsequent analysis and use of those data.[379]

6. Matching or combining datasets, [*in particular if they*] originat[*e*] from two or more data processing operations performed for different purposes and/or [*are carried out*] by different data controllers in a way that would exceed the reasonable expectations of the data subject.

---

[376] The relative clarification in Recital 91 reads: "*[L]arge-scale processing operations [are operations] which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, [or] where in accordance with the achieved state of technological knowledge a new technology is used on a large scale ...*"

[377] This example is taken from the **Italian** DPIA list approved by the EDPB.

[378] Cf. the decision of the French DPA (the *CNIL*) on the Mormon's genealogical register, issued in 2013 and reported here: https://www.nouvelobs.com/societe/20130613.OBS3162/les-mormons-autorises-par-la-cnil-a-numeriser-l-etat-civil-francais.html

[379] This practice is common and indeed traditional in the UK, as is recognised in Recital 56 of the GDPR. That recital says that "this *may* be permitted for reasons of public interest, *provided that appropriate safeguards are established*" (emphases added). If anything, this need to assess whether the processing really serves a legitimate public interest and the requirement to adopt "appropriate safeguards" underline the need for a serious risk analysis and impact assessment.

Example:

Covertly cross-checking access control logs, computer logs and flexitime declarations [*by an employer*] to detect absenteeism.*

A tax office matches its records of tax returns against records of owners of expensive yachts, to look for people who may possibly be committing tax fraud.[380]

7. Data concerning vulnerable data subjects (recital 75): the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include **children** (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), **employees** , more vulnerable segments of the population requiring special protection (**mentally ill persons**, **asylum seekers**, or the **elderly**, **patients**, etc.), and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.

Examples:

Use of video surveillance and geolocation systems enabling the distance monitoring of employees' activities.[381]

Essentially any processing of personal data on any of the above categories of vulnerable persons, and certainly any processing of sensitive data on them, or large-scale processing of such data on such people, should be considered as inherently likely to result in a "high risk".

8. Innovative use or applying new technological or organisational solutions. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology, defined in "accordance with the achieved state of technological knowledge" (recital 91), can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms or types of data collection and usage, possibly invisible and with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks – and the mitigating measures should make it possible for data subjects and the general public to see how and when and for what purposes the new technologies are to be used, so that they can guard against those that can undermine individual rights and freedoms and lead to authoritarian government or mass-surveillance by corporations (or those acting together).

   Note: In many such cases of new technologies or practices, the DPAs (or the EDPB) may issue, or may already have issued, opinions, guidelines or recommendations – and DPOs should be on the alert to watch out for such new documents. If they believe that no relevant guidance etc. has yet been issued, they should consult their DPA. See also Tasks 4, 8 and 10, below.

---

380 This was done some time ago in the Netherlands, on the assumption that large yachts were typically bought by tax fraudsters. One person, feeling himself targeted, tauntingly called his ship "*Black Money*".

381 This example is taken from the **Italian** DPIA list approved by the EDPB.

Examples:

Combining use of finger print and face recognition for improved physical access control.[382]

New technologies intended to track employees' time and attendance, including those that process of biometric data as well as others such as mobile device tracking.[383]

Processing of data generated through the use of "Internet of Things" applications (*connected, "smart" devices and things*) if the use of the data has (or can have) a significant impact on individuals' daily lives and privacy.

Machine learning.*

Connected cars.*

Social media screening of applicants for posts.*

9. When the processing in itself "*prevents data subjects from exercising a right or using a service or a contract*" (Article 22 and recital 91). This includes processing operations that aim at allowing, modifying or refusing data subjects' access to a service or entry into a contract.

Examples:

A bank screening its customers against a credit reference database in order to decide whether to offer them a loan.

A financial institution or credit reference agency taking into account the age difference between spouses in a marriage to determine creditworthiness (which can impede the free exercise of the fundamental right to marriage – and was therefore prohibited in France by the French DPA, the CNIL (which had to assess the system because, since it took decisions bases on profiles, was subject to "prior authorisation" by the CNIL).

Exclusion databases.*

Credit screening.*

Multi-factor high-risk operations

The factors listed above can overlap or be combined, e.g., "systematic monitoring" can overlap with, and be combined with, automated profile-based decision-making, and may involve "large-scale" processing of "sensitive data". The WP29 provides a number of examples of operations with such combined factors (or criteria) for which a DPIA is required, and examples of operations in which one or more of the above factors (or criteria) are present, but where no DPIA is needed, as follows:[384]

---

382 The WP29 and several national DPAs have issued detailed advice on this requiring, among other matters, that the biological data should be stored on the micro-processing chip in the data subject's device, rather than centrally by the controller. See: WP29 Working document on biometrics (WP80, adopted on 1 August 2003), p. 6, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf

383 See WP29 Opinion 2/2017 on data processing at work (WP249, adopted on 8 June 2017), section 5.5, *Processing operations relating to time and attendance*, at pp. 18 – 19, available at: www.ec.europa.eu/newsroom/document.cfm?doc_id=45631

384 WP29 Guidelines on DPIAs (footnote 351, above), pp. 11 – 12.

Examples of processing	Possible Relevant criteria	DPIA likely to be required?
A hospital processing its patients' genetic and health data (hospital information system).	- Sensitive data or data of a highly personal nature. - Data concerning vulnerable data subjects. - Data processed on a large-scale.	Yes
The use of a camera system to monitor driving behaviour on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates.	- Systematic monitoring. - Innovative use or applying technological or organisational solutions.	
A company systematically monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc.	- Systematic monitoring. - Data concerning vulnerable data subjects.	
The gathering of public social media data for generating profiles.	- Evaluation or scoring. - Data processed on a large scale. - Matching or combining of datasets. - Sensitive data or data of a highly personal nature:	
An institution creating a national level credit rating or fraud database.	- Evaluation or scoring. - Automated decision making with legal or similar significant effect. - Prevents data subject from exercising a right or using a service or a contract. - Sensitive data or data of a highly personal nature:	
Storage for archiving purpose of pseudonymised personal sensitive data concerning vulnerable data subjects of research projects or clinical trials	- Sensitive data. - Data concerning vulnerable data subjects. - Prevents data subjects from exercising a right or using a service or a contract.	
A processing of "personal data from patients or clients by an individual physician, other health care professional or lawyer" (Recital 91).	- Sensitive data or data of a highly personal nature. - Data concerning vulnerable data subjects.	No
An online magazine using a mailing list to send a generic daily digest to its subscribers with their consent, and which includes an easy means to opt out of further mailings.	- Data processed on a large scale.	
An e-commerce website displaying adverts for vintage car parts involving limited profiling based on items viewed or purchased on its own website – again, with an easy opt-out facility.	- Evaluation or scoring.	

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Methodologies for DPIAs:

The aims of a DPIA are:

(i) to precisely **identify** the (high) risks involved in the proposed processing operation, taking into account the nature of the data and the processing, the scope, context and purposes of the processing and the sources of the risk – not only in normal circumstances, but also in special circumstances; and in the short-, medium- and long term;[385]

(ii) to **evaluate** the identified (high) risks, in particular its origin, nature, and particularity, and the likelihood and possible severity of the risk;[386]

(iii) to identify what **measures** can be taken to mitigate the (high) risks that are appropriate in terms of available technology and costs of implementation, and to propose such measures;[387] and

(iv) to **record** the findings, evaluation and measures taken (or not taken, with the reasons for that), so as to be able to "**demonstrate compliance**" with the requirements of the GDPR under the "accountability" principle in relation to the assessed processing.[388]

Article 35(7) GDPR stipulates that (the record of) a DPIA must contain "at least" the following:

> (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
>
> (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
>
> (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
>
> (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

The WP29 stresses that:[389]

> All the relevant requirements set out in the GDPR provide a broad, generic framework for designing and carrying out a DPIA. The practical implementation of a DPIA will depend on the requirements set out in the GDPR which may be supplemented with more detailed practical guidance. **The DPIA implementation is therefore scalable. This means that even a small data controller can design and implement a DPIA that is suitable for their processing operations.**

---

385 Cf. Recital 90.

386 Cf. Recital 84 and ISO 31000.

387 Cf. Recital 84.

388 As the WP29 puts it: "*[A] DPIA is a process for building and demonstrating compliance.*" – WP29 Guidelines on DPIAs (footnote 351, above), p. 4. For further detail on the accountability principle and the associated "demonstration of compliance" duties, see Part 2 of the handbook.

389 WP29 Guidelines on DPIAs (footnote 351, above), p. 17, emphasis added.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Controllers can therefore (in consultation with their DPO) choose a methodology for any DPIA they have to carry out that suits them. They can draw on any experience they may have with more technical risk assessments, e.g., under ISO 31000. However, the WP29 rightly note the different perspective from which DPIAs are to be carried out under the GDPR and the (in any case, more narrowly security-oriented) ISO-based assessments:[390]

> [T]he DPIA under the GDPR is a tool for managing risks to the rights of the data subjects, and thus takes their [i.e., the data subjects'] perspective … Conversely, risk management in other fields (e.g. information security) is focused on the [risks to the] organization.

The WP29 provides a number of examples of data protection and privacy impact methodologies prepared by national DPAs,[391] and "*encourages the development of sector-specific DPIA frameworks*". It has itself published a DPIA Framework for RFID Applications and a DPIA Template for Smart Grid and Smart Metering Systems.[392]

Here, it must suffice to reproduce the Criteria for an acceptable DPIA, set out in the WP29 guidelines:[393]

Annex 2 – Criteria for an acceptable DPIA

> The WP29 proposes the following criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR:
>
> - **a systematic description of the processing is provided**(Article 35(7)(a))**:**
> - nature, scope, context and purposes of the processing are taken into account (Recital 90);
> - personal data, recipients and period for which the personal data will be stored are recorded;
> - a functional description of the processing operation is provided;
> - the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
> - compliance with approved codes of conduct [*, certifications and/or BCRs*][394] is taken into account (Article 35(8));
> - **necessity and proportionality are assessed**(Article 35(7)(b))**:**
> - measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:

---

390 *Idem*.

391 See again the list with links in *Annex 1* to the WP29 Guidelines on DPIAs (footnote 351, above).

392 *Idem*, footnotes 32 and 33.

393 *Idem*, Annex 2. The emphases in bold in the main bullet-points have been added for clarity.

394 The WP29 notes earlier that:

"*Compliance with a code of conduct (Article 40) has to be taken into account (Article 35(8)) when assessing the impact of a data processing operation. This can be useful to demonstrate that adequate measures have been chosen or put in place, provided that the code of conduct is appropriate to the processing operation. Certifications, seals and marks for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors (Article 42), as well as Binding Corporate Rules (BCR), should be taken into account as well.*"
WP29 Guidelines on DPIAs (footnote 351, above), p. 16.

- measures contributing to the proportionality and the necessity of the processing on the basis of:
  - specified, explicit and legitimate purpose(s) (Article 5(1)(b));
  - lawfulness of processing (Article 6);
  - adequate, relevant and limited to what is necessary data (Article 5(1)(c));
  - limited storage duration (Article 5(1)(e));
- measures contributing to the rights of the data subjects:
  - information provided to the data subject (Articles 12, 13 and 14);
  - right of access and to data portability (Articles 15 and 20);
  - right to rectification and to erasure (Articles 16, 17 and 19);
  - right to object and to restriction of processing (Article 18, 19 and 21);
  - relationships with processors (Article 28);
  - safeguards surrounding international transfer(s) (Chapter V);
  - prior consultation (Article 36).

- **risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):**

- origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
  - risks sources are taken into account (recital 90);
  - potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
  - threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
  - likelihood and severity are estimated (recital 90);
- measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);

- **interested parties are involved:**

- the advice of the DPO is sought (Article 35(2));
- the views of data subjects or their representatives are sought, where appropriate (Article 35(9)).

What to do with the record of the DPIA

The first and main purpose of the record of the DPIA (covering all of the above "criteria") is to have **evidence** that a proper, in-depth DPIA has been carried out, in accordance with the GDPR (i.e., meeting the above criteria).

Where the DPIA identifies at the same time both (high) risks and measures that can be taken to address those risks that are "appropriate" taking into account the likelihood and severity of the risks and the costs of the measures, and where such measures have indeed been approved and adopted (and this approval and adoption, too, has been recorded), the DPIA record can provide **an important "element" in an overall demonstration of**

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

compliance and a "special means" to do this (although this does not amount to a legal presumption of compliance, and although the DPO will still have to **check and monitor**, on an ongoing basis, that the mitigating measures continue to be applied and continue to be appropriate in the light of practical, organisational or technological developments: see under this Task, under the heading "*Ongoing monitoring of compliance*").

Examples of **cases where the DPIA identified both the high risks and the mitigation measures, which were considered (*in casu*, by EuroPrise) to be sufficient to allow the processing. Consequently, both cases would enable the controller to confidently conclude that the outcome of the DPIA shows that the processing would NOT need to be submitted to the competent DPA for consultation:**[395]

1. A welfare agency uses voice biometric authentication to counter welfare fraud.

Identification of risks: As the WP29 has pointed out, three of the main risks posed by the use of biometric data are: (i) the fact that a person's biometric features are irreplaceable (which means that an authentication tool based on raw biometric data, once lost, cannot be replaced); (ii) the ease with which biometric data can be used to match different datasets; and (iii) the possibility that biometric data can be captured surreptitiously.

Mitigation measures: In a (voice) biometric authentication tool, used to counter welfare fraud, a unique voice *template* is used, created from the original ("raw") biometric data, rather than the raw data, which are destroyed after enrolment of the data subjects. The voice template is unique to any specific deployment, and it cannot be used to re-create the original (raw) biometric data. This addresses all three of the above-mentioned risks: (i) if the voice template were to be compromised, a new, different one can be created very simply (with the help of the data subject, who would need to be re-enrolled); (ii) the different voice templates used in different deployments of the same tool cannot be matched against each other or against other voice data or voice templates; and (iii) the voice template is created in a face-to-face enrolment process.

2. A financial institution checks the location of a customer's mobile phone to see if it is (roughly) in the same place as the customer's bank card (which is being used for a transaction that has been flagged up as suspicious).

Identification of risks: Precise details of someone's location at a particular time can be highly revealing of sensitive matters, and the revelation of those details therefore constitutes a serious interference with the privacy and private life of the individual concerned – as the European Court of Human Rights confirmed in the *Naomi Campbell* case.[396]

Mitigation measures: In the bank card fraud-prevention tool, the location data of the mobile phone are reduced, even before being passed on to the user of that tool (the financial institution), to a very rough area, typically a country or state. That is sufficient for the tool to work efficiently (i.e., being able to ascertain with sufficient certainty whether or not the transaction in question is genuine or fraudulent), while reducing the intrusiveness of the location check to the absolute minimum.

---

[395] These examples are taken from products that have obtained the European Privacy Seal, with the legal evaluations done by Douwe Korff, see, respectively:
https://www.european-privacy-seal.eu/EPS-en/4F-self-certification (a four-factor authentication tool that includes a voice biometric solution);
https://www.european-privacy-seal.eu/eps-en/valid-pos (a tool that matches the location of a suspicious bank card transaction with the (rough) location of the card holder's mobile phone).
In the evaluations, both products were praised for their extensive data minimisation and privacy-by-design features, and for the way in which those mitigated the risks associated with, respectively, the use of biometric data and location checking.

[396] ECtHR, *MGN v. the UK*, judgment of 18 January 2011, available at:
https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-102965%22]}

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

The record can also be made available (or drawn on) in **consultations** involving concerned parties or citizens, or in responses to **queries and complaints from data subjects and non-governmental organisations** representing data subjects (or the press). In that respect, the WP29 observes that:[397]

> **Publishing a DPIA is not a legal requirement of the GDPR, it is the controller´s decision to do so. However, controllers should consider publishing at least parts, such as a summary or a conclusion of their DPIA.**
>
> The purpose of such a process would be to help foster trust in the controller's processing operations, and demonstrate accountability and transparency. ***It is particularly good practice to publish a DPIA where members of the public are affected by the processing operation. This could particularly be the case where a public authority carries out a DPIA.***
>
> The published DPIA does not need to contain the whole assessment, especially when the DPIA could present specific information concerning security risks for the data controller or give away trade secrets or commercially sensitive information. In these circumstances, the published version could consist of just a summary of the DPIA's main findings, or even just a statement that a DPIA has been carried out.

The DPIA record is of particular importance in dealing with any queries from DPAs, whether acting in their general supervisory capacity or in response to a complaint.

More specifically, where the DPIA identifies at the same time both (high) risks and finds that there are **no** measures that can be taken to sufficiently address all those risks (or at least no measures that are "appropriate" taking into account the likelihood and severity of the risks and the costs of the measures), the controller is required to **consult the DPA** (Art. 36) – and **the record of the relevant DPIA must be provided to the DPA**:[398]

> where a DPIA reveals high residual risks, the data controller will be required to seek prior consultation for the processing from the supervisory authority (Article 36(1)). As part of this, the DPIA must be fully provided (Article 36(3)(e)). The supervisory authority may provide its advice,[399] and will not compromise trade secrets or reveal security vulnerabilities, subject to the principles applicable in each Member State on public access to official documents.

Member States may also, under their **national law**, require controllers to consult the DPA "in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health" (Art. 36(5)), and this has been done for those latter cases in. e.g., France and Italy.

If the DPA is not satisfied with the information in the DPIA record (and/or otherwise provided), the DPA can **order** the controller to provide any further information it feels it requires to assess the matter (Cf. Art. 58(1)(a)).

Usually, the DPA will try to **help** the controller find a solution – i.e., identify measures that would adequately mitigate the identified (high) risks (in the opinion of the DPA), and

---

397 WP29 Guidelines on DPIAs (footnote 351, above) p. 18, emphasis in bold original, emphasis in italics and bold added.

398 *Idem*.

399 Written advice to the controller is only necessary when the supervisory authority is of the opinion that the intended processing is not in line with the regulation as per Article 36(2). [original footnote]

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

provided that the controller agrees to adopt those measures (and that their adoption and continuing use is checked and monitored by the DPO), that would resolve the matter (as should be recorded by the DPO and will of course also be recorded by the DPA).

But alternatively, the DPA can either issue an **order** to the controller, requiring the controller to adopt specified measures for the proposed processing operation (Cf. Art. 58(2)(d)), or indeed **prohibiting** the proposed processing (Art. 58(2)(f)).

The DPO should of course again record any such orders, and check on an on-going basis that they are complied with (and record her findings). But as always, apart from this checking, monitoring and record keeping, it is ultimately the controller who will be held to account for any failure to comply.

- o – O – o –

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Monitoring of compliance (including investigations of complaints):

TASK 5: Repeating Tasks 1 – 3 (and 4) on an ongoing basis

As the WP29 points out in its (EDPB-endorsed) Guidelines on DPOs, Article 39(1)(b) entrusts the DPO, among other duties, with the duty to "monitor compliance" of her organisation with the GDPR, andRecital 97 further specifies that DPO "should assist the controller or the processor to monitor internal compliance with this Regulation".[400] As the very term "monitor" indicates, this is not a one-off but an ongoing responsibility.

However, in line with our discussion on the role of the DPO in Part 2, section 2.3.4, above, the WP29 also (again) stressed that this:[401]

> does not mean that it is the DPO who is personally responsible where there is an instance of non-compliance. The GDPR makes it clear that it is the controller, not the DPO, who is required to '*implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation*' (Article 24(1)). Data protection compliance is a corporate responsibility of the data controller, not of the DPO.

The WP29 goes on to say that as part of these duties to monitor compliance, DPOs may, in particular, on an on-going basis:

- collect information to identify processing activities,
- analyse and check the compliance of processing activities, and
- inform, advise and issue recommendations to the controller or the processor.

As it notes in relation to DPIAs (Task 4):[402]

> It has to be stressed that in order to manage the risks to the rights and freedoms of natural persons, the risks have to be identified, analysed, estimated, evaluated, treated (e.g. mitigated...), **and reviewed regularly**.

In other words, Tasks 1 – 4, above (or if there are no likely "high risk" operations, Tasks 1 – 3), are to be repeated on an on-going basis, and in particular of course if the organisation changes any personal data processing operation, or implements any new ones. As the EDPS puts it (in his advice to EU institutional DPOs):[403]

> Your records have to reflect the reality of your [institution's] processing operations. This means that you have to ensure they are up-to-date. When [your institution is] planning changes to your processing operations, check if the record needs updating. It is a good idea to formally include this check in your change management process. It may also be a good idea to conduct regular reviews independently of planned changes in order to catch changes that may have gone unnoticed.

The WP29 has illustrated the last part of this sequence in a useful diagram, reproduced overleaf, with the earlier stages (Tasks 2 and 3) added.

---

400 WP29 Guidelines on DPOs (footnote 242, above), section 4.1, *Monitoring compliance with the GDPR*, on p. 16,7.

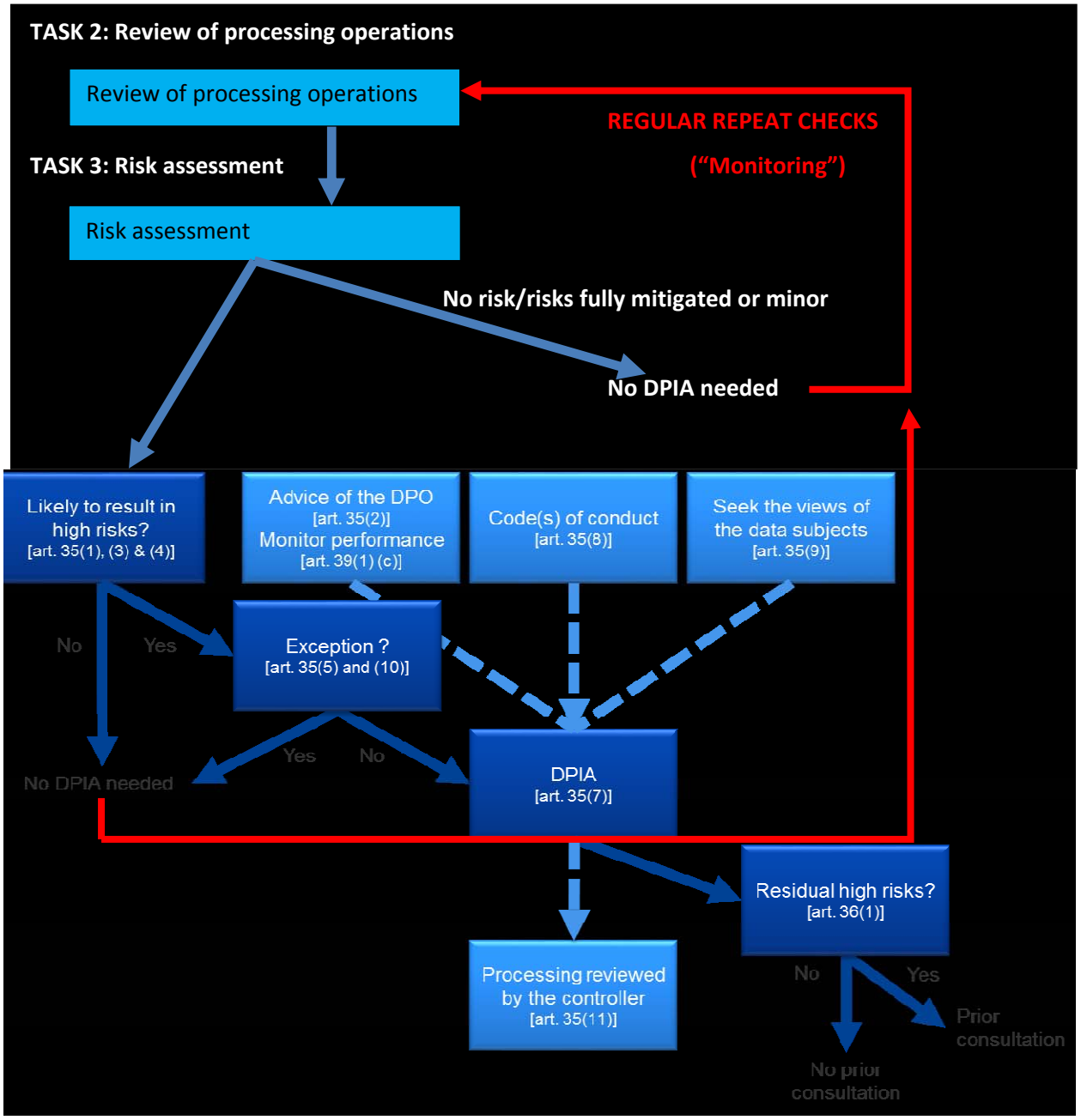
401 *Idem*, original italics.

402 WP29 Guidelines on DPIAs (footnote 351, above), footnote 10 on p. 6, emphasis added.

403 EDPS, Accountability on the ground (footnote 353, above).

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

WP29 diagram on the steps to be followed in relation to DPIAs,[404] with the earlier steps (Tasks 2 and 3) added in the top box:



Note: The exceptions under Art. 35(5), noted in the WP29 diagram, relate to national security, defence, crime prevention, etc. Art. 35(10) concerns the stipulation that no DPIA is required in relation to processing regulated by law, if a general DPIA of that processing has been carried out in the lead-up to the law (which does not involve the DPO).

As part of her "monitoring of compliance" duties, the DPO should also make sure she is aware in any changes in the regulatory and contractual (etc.) framework within which her organisation operates, as scoped in the preliminary task (Task 0), so that she is able to identify the impact on any such changes on (the ongoing legality and GDPR-compliance of) her organisation's personal data processing operations, and can issue appropriate advice to the relevant persons in her organisation (including top management where appropriate).

404 WP29 Guidelines on DPIAs (footnote 351, above), p. 7.

Indeed, the DPO should – where appropriate together with other DPOs in her DPO network and/or with the DPA, and in consultation with her top management – at times be willing to adopt positions and views on proposed or suggested changes to this framework, such as proposals by a government that organisations such as hers should be required, enabled or encouraged to share certain personal data for new purposes.

- o – O – o –

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

TASK 6: Dealing with personal data breaches

Two of the main, important innovations brought in by the GDPR compared to the 1995 Data Protection Directive, are (i) a general requirement to notify the relevant (i.e., "competent") DPA of any personal data breach that may result in a risk to the rights and freedoms of individuals; and (ii) a duty to inform data subjects of such breaches in casesin which the brach is likely to result in a "high risk" to the rights and freedoms of natural persons.

The Article 29 Working Party has issued detailed guidelines on how personal data breaches should be handled;[405] and this guidance was endorsed by the European Data Protection Board at its first meeting.[406] The discussion, below, will extensively draw on and refer to these guidelines. The examples provided are also all taken from these WP29 Guidelines.[407]

Notifying the relevant DPA:

The idea of notification of personal data breaches is not new. As noted in section 1.3.3, above,[408] a personal data breach notification duty was already included in the e-Privacy Directive. However, that duty was limited to providers of electronic communications networks and -services.[409]The GDPR uses the samedefinition of "*personal data breach*" as is contained in the e-Privacy Directive, but without this limitation:

> a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. (Art. 4(12))[410]

The WP29 Guidelines clarify in some detail what the relevant terms should be taken as meaning, and sets out the different types of personal data breaches ("*confidentiality breach*"; "*integrity breach*"; "*availability breach*")[411]

> **Examples**
>
> An example of loss of personal data can include where a device containing a copy of a controller's customer database has been lost or stolen. A further example of loss may be where the only copy of a set of personal data has been encrypted by ransomware (malicious software which encrypts the controller's data until a ransom is paid), or has been encrypted by the controller using a key that is no longer in its possession.
>
> Examples of a loss of availability include where data has been deleted either accidentally or by an unauthorised person, or, in the example of securely encrypted data, the decryption key has been lost. In the event that the controller cannot restore

405 WP29, Guidelines on Personal data breach notification under Regulation 2016/679 (WP250 rev.01, adopted on 3 October 2017, as last revised and adopted on 6 February 2018 (hereafter: "WP29 Guidelines on Data Breach Notification or, in this section, simply "the WP29 Guidelines"), available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

406 See footnote 248, above.

407 The WP29 Guidelines also discuss notification obligations under other legal instruments: see Section VI of the Guidelines. These are not further discussed here.

408 In the sub-section on "*Key features of the e-Privacy Regulation*", under the sub-heading "Data breach notification".

409 As the WP29 Guidelines note in the Introduction, some Member States also already had wider data breach notification requirements.

410 The e-Privacy Directive added after these same words, the words: "*in connection with the provision of a publicly available electronic communications service in the Community*" (art. 2(i)).

411 WP29 Guidelines, p. 7, with reference to an earlier (2014) WP29 Opinion on breach notification.

access to the data, for example, from a backup, then this is regarded as a permanent loss of availability.

A loss of availability may also occur where there has been significant disruption to the normal service of an organisation, for example, experiencing a power failure or denial of service attack, rendering personal data unavailable.

Even a temporary loss of availability can constitute a personal data breach:

Examples

In the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals' rights and freedoms; for example, operations may be cancelled and lives put at risk.

Conversely, in the case of a media company's systems being unavailable for several hours (e.g. due to a power outage), if that company is then prevented from sending newsletters to its subscribers, this is unlikely to present a risk to individuals' rights and freedoms.

Infection by ransomware could lead to a temporary loss of availability if the data can be restored from backup. However, a network intrusion still occurred, and notification could be required if the incident is qualified as confidentiality breach (i.e. personal data is accessed by the attacker) and this presents a risk to the rights and freedoms of individuals.

Article 33(1) stipulates that:

> In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. (Article 33(1)).

A processor must "*notify the controller without undue delay after becoming aware of a personal data breach*" (Art. 33(2)). The WP29 recommends that the processor:

> **promptly** notifies the controller, with further information about the breach provided in phases as more details become available. This is important in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours. (WP29 Guidelines, p. 14)

The controller will be regarded as "**aware**" of the breach once the processor informed him of this;[412] andthe controller must then notify the DPA (as mentioned), unless the *caveat*that the data breach is unlikely to result in a risk to the rights and freedoms of natural persons applies.

In certain cases, a processor may be acting for a number – perhaps even a large number – of different controllers, for instance as a cloud data storage provider. The WP29 advises as follows for such situations:

412 WP Guidelines, p. 14.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

> Where the processor provides services to multiple controllers that are all affected by the same incident, the processor will have to report details of the incident to each controller.
>
> A processor could make a notification on behalf of the controller, if the controller has given the processor the proper authorisation and this is part of the contractual arrangements between controller and processor. Such notification must be made in accordance with Article 33 and 34. However, it is important to note that the legal responsibility to notify remains with the controller. (p.14)

The notification of the data breach to the relevant ("competent") DPA[413] "shall at least":

> a. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
>
> b. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
>
> c. describe the likely consequences of the personal data breach;
>
> d. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
>
> (Art. 33(3))

In that respect, the WP29 says that the controller can:[414]

> if necessary, choose to provide further details. Different types of breaches (confidentiality, integrity or availability) might require further information to be provided to fully explain the circumstances of each case.

> **Example**
>
> As part of its notification to the supervisory authority, a controller may find it useful to name its processor if it is at the root cause of a breach, particularly if this has led to an incident affecting the personal data records of many other controllers that use the same processor.

> In any event, the supervisory authority may request further details as part of its investigation into a breach.

Moreover:

> Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. (Art. 33(4))[415]

> **Example**
>
> A controller notifies the supervisory authority within 72 hours of detecting a breach that it has lost a USB key containing a copy of the personal data of some of its customers. The USB key is later found misfiled within the controller's premises and recovered. The controller updates the supervisory authority and requests the notification be amended.

---

413 For guidance on the notification of cross-border breaches and of breaches taking place at non-EU establishments, see section C in the WP29 Guidelines (pp. 16 – 18).

414 WP29 Guidelines, p. 15.

415 For details and further guidance on this issue, see the WP29 Guidelines, pp. 15 – 16.

Timing of the notification:

The WP29 Guidelines clarify when a controller (or a processor) can be said to have become "**aware**" of a data breach, and stresses that there are also duties to anticipate and prepare for such an event:[416]

> As detailed above, the GDPR requires that, in the case of a breach, the controller shall notify the breach without undue delay and, where feasible, not later than 72 hours after having become aware of it. This may raise the question of when a controller can be considered to have become "aware" of a breach. WP29 considers that a controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.
>
> However, as indicated earlier, the GDPR requires the controller to implement all appropriate technical protection and organisational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject21. This puts an obligation on the controller to ensure that they will be "aware" of any breaches in a timely manner so that they can take appropriate action.
>
> When, exactly, a controller can be considered to be "aware" of a particular breach will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.

Examples

1. In the case of a loss of a USB key with unencrypted personal data it is often not possible to ascertain whether unauthorised persons gained access to that data. Nevertheless, even though the controller may not be able to establish if a confidentiality breach has taken place, such a case has to be notified as there is a reasonable degree of certainty that an availability breach has occurred; the controller would become "aware" when it realised the USB key had been lost.

2. A third party informs a controller that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure. As the controller has been presented with clear evidence of a confidentiality breach then there can be no doubt that it has become "aware".

3. A controller detects that there has been a possible intrusion into its network. The controller checks its systems to establish whether personal data held on that system has been compromised and confirms this is the case. Once again, as the controller now has clear evidence of a breach there can be no doubt that it has become "aware".

4. A cybercriminal contacts the controller after having hacked its system in order to ask for a ransom. In that case, after checking its system to confirm it has been

[416] WP29 Guidelines, pp. 10 – 11.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

attacked the controller has clear evidence that a breach has occurred and there is no doubt that it has become aware.

5. An individual informs the controller that they have received an email impersonating the controller which contains personal data relating to his (actual) use of the controller's service, suggesting that the security of the controller has been compromised. The controller conducts a short period of investigation and identifies an intrusion into their network and evidence of unauthorised access to personal data. The controller would now be considered as "aware" and notification to the supervisory authority is required unless this is unlikely to present a risk to the rights and freedoms of individuals. The controller will need to take appropriate remedial action to address the breach.

Documenting and assessing the breach:

The GDPR also stipulates that:

> The controller shall document **any** personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article. (Art. 33(5), emphasis added)

Note that this latter requirement relates to **all** ("any") personal data breach: it is not limited to data breaches of which the DPA has to be notified, i.e., the record must also include any data breaches that (in the opinion of the controller) were "unlikely to result in a risk to the rights and freedoms of natural persons".

In practice, the DPO will have to be closely and deeply involved in these matters. Often, a suspected breach is likely to be first reported internally to her (and/or to the Chief Technology- or Security Officer) – and the DPO must then (as appropriate, with those other officers) make the first, immediate assessment of at least the following matters:

- whether there actually has been a personal data breach as defined in the GDPR (see the definition in Article 4(12), quoted above) –

  and if it is established that there was a breach, or that it is likely that there may have been a breach:

- which (categories of) data subjects were or may have been affected by the breach and what (categories of) personal data may have been lost or otherwise affected –

  NB: The WP29 recommends that these categories also be reported to the DPA in any breach notification, and indeed that:[417]

  > if the types of data subjects or the types of personal data indicate a risk of particular damage occurring as a result of a breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy), then it is important the notification indicates these categories. In this way, it is linked to the requirement of describing the likely consequences of the breach.

  and taking those matters into account:

- whether the breach is "likely" or "unlikely" to result in a risk to the rights and freedoms of natural persons –

[417] WP29 Guidelines, p. 14.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

The WP29 discusses the question of when notification is not required in some detail[418] and provides the following example:

> **Example**
>
> A breach that would not require notification to the supervisory authority would be the loss of a securely encrypted mobile device, utilised by the controller and its staff. Provided the encryption key remains within the secure possession of the controller and this is not the sole copy of the personal data then the personal data would be inaccessible to an attacker. This means the breach is unlikely to result in a risk to the rights and freedoms of the data subjects in question. If it later becomes evident that the encryption key was compromised or that the encryption software or algorithm is vulnerable, then the risk to the rights and freedoms of natural persons will change and thus notification may now be required.

*but if the assessment is that there **is** a likelihood of such a potential risk:*

- whether the risk is a "high risk to the rights and freedoms of [those] natural persons" (because that would require not just notification of the breach to the DPA, but also the informing of the data subjects, as noted under the next sub-heading).[419]

As the WP29 points out, the importance of being able to identify a breach, to assess the risk to individuals, and then notify if required, is emphasised in Recital 87 of the GDPR:

> It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

And of course, if the assessments indicate that there was a breach, and that there are risks to the interests of individuals, then **mitigating measures** should be urgently sought.

The above matters should also**urgently, at the earliest possible moment**, be passed on to highest management. Indeed, any internal discussions of the above matters should not delay the informing of highest management as soon as a breach is established.

The fact that those assessments were done, conscientiously, should be **carefully recorded**,[420] together with the outcomes of the relevant assessments and the reasons for those assessments; the mitigating measures considered; the fact that the assessments and the proposed mitigating measures were communicated to highest management; the actual measures authorised by management and whether, and when, they were carried out; and of course, the fact that the breach (if found to be notifiable) was notified to the relevant DPA(s) and when, with a copy of the notification; and where required, the fact that data

---

418 WP29 Guidelines, pp. 18 – 19. See also the non-exhaustive list of examples provided in an annex (Annex B) to the Guidelines, reproduced below, under the next sub-heading.

419 See in particular the discussion under the sub-heading "*Assessing risk and high risk*".

420 The WP29 suggests, that this be done "*in the controller's incident report plan and/or governance arrangements*" (p. 12). This is further discussed in some detail in the WP29 Guidelines, Section V, *Accountability and record-keeping*".

subjects were informed, and how, with a copy of the relevant notification and any relevant press release, etc. (as discussed under the next heading).Moreover, as the WP29 Guidelines say:

> Documentation of the breach should take place as it develops (p. 12).

In organisations that have appointed a DPO, she will have an important role to play in these regards, as the WP29 stresses:[421]

> A controller or processor may have a Data Protection Officer (DPO)48, either as required by Article 37, or voluntarily as a matter of good practice. Article 39 of the GDPR sets a number of mandatory tasks for the DPO, but does not prevent further tasks being allocated by the controller, if appropriate.
>
> Of particular relevance to breach notification, the mandatory tasks of the DPO includes, amongst other duties, providing data protection advice and information to the controller or processor, monitoring compliance with the GDPR, and providing advice in relation to DPIAs. The DPO must also cooperate with the supervisory authority and act as a contact point for the supervisory authority and for data subjects. It should also be noted that, when notifying the breach to the supervisory authority, Article 33(3)(b) requires the controller to provide the name and contact details of its DPO, or other contact point.
>
> In terms of documenting breaches, the controller or processor may wish to obtain the opinion of its DPO as to the structure, the setting up and the administration of this documentation. The DPO could also be additionally tasked with maintaining such records.
>
> These factors mean that the DPO should play an key role in assisting the prevention of or preparation for a breach by providing advice and monitoring compliance, as well as during a breach (i.e. when notifying the supervisory authority), and during any subsequent investigation by the supervisory authority. In this light, WP29 recommends that the DPO is promptly informed about the existence of a breach and is involved throughout the breach management and notification process.

The WP29 Guidelines make clear that organisations should not just be reactive in this regard. Rather, they should have a **security policy** in place that ***in advance*** seeks to avoid any data breaches, and contains plans to prevent, mitigate and end them. In relation to personal data processing operations likely to result in a "high risk" to the interests of individuals, the designing of such a policy can be part of a relevant Data Protection Impact Assessment (as discussed in Task 4, above).[422]

Informing the data subjects:

The WP29 clarifies the requirements on the informing of data subjects of a data breach as follows:

> In certain cases, as well as notifying the supervisory authority, the controller is also required to communicate a breach to the affected individuals.
>
> Article 34(1) states:

421 WP29 Guidelines, Section V.B, pp. 27 – 28.

422 WP29 Guidelines, p. 6.

> When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

Controllers should recall that notification to the supervisory authority is mandatory unless there is unlikely to be a risk to the rights and freedoms of individuals as a result of a breach. In addition, where there is likely a high risk to the rights and freedoms of individuals as the result of a breach, individuals must also be informed. The threshold for communicating a breach to individuals is therefore higher than for notifying supervisory authorities and not all breaches will therefore be required to be communicated to individuals, thus protecting them from unnecessary notification fatigue.

The GDPR states that communication of a breach to individuals should be made "without undue delay," which means as soon as possible. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves36. As noted above, depending on the nature of the breach and the risk posed, timely communication will help individuals to take steps to protect themselves from any negative consequences of the breach.

An annex (Annex B) to the WP29 Guidelines, which provides a (non-exhaustive) list of 10 examples of personal data breaches and who should be notified, is attached to the discussion of the present task as an Attachment.

The WP29 Guidelines continue as follows:[423]

Information to be provided

When notifying individuals, Article 34(2) specifies that:

> The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

According to this provision, the controller should at least provide the following information:

- a description of the nature of the breach;
- the name and contact details of the data protection officer or other contact point;
- a description of the likely consequences of the breach; and
- a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

Example:

As an example of the measures taken to address the breach and to mitigate its possible adverse effects, the controller could state that, after having notified the breach to the relevant supervisory authority, the controller has received advice on managing the breach and lessening its impact. The controller should also, where appropriate, provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords in the case where

423 Section III.B, p. 20. Text edited for presentation only.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

their access credentials have been compromised. Again, a controller can choose to provide information in addition to what is required here.

The Guidelines also clarify that:[424]

> In principle, the relevant breach should be communicated to the affected data subjects directly, unless doing so would involve a disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner (Article 34(3)c).

The communications to data subjects should be made "as soon as reasonably feasible and in close cooperation with the supervisory authority" (Recital 86). As the Guidelines note:[425]

> Controllers might therefore wish to contact and consult the supervisory authority not only to seek advice about informing data subjects about a breach in accordance with Article 34, but also on the appropriate messages to be sent to, and the most appropriate way to contact, individuals.
>
> Linked to this is the advice given in Recital 88 that notification of a breach should "take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach". This may mean that in certain circumstances, where justified, and on the advice of law-enforcement authorities, the controller may delay communicating the breach to the affected individuals until such time as it would not prejudice such investigations. However, data subjects would still need to be promptly informed after this time.
>
> Whenever it is not possible for the controller to communicate a breach to an individual because there is insufficient data stored to contact the individual, in that particular circumstance the controller should inform the individual as soon as it is reasonably feasible to do so (e.g. when an individual exercises their Article 15 right to access personal data and provides the controller with necessary additional information to contact them).

Exceptions:

As the WP29 Guidelines note:[426]

> Article 34(3) states three conditions that, if met, do not require notification to individuals in the event of a breach. These are:
>
> - The controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it. This could, for example, include protecting personal data with state-of-the-art encryption, or by tokenization.
> - Immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise. For example, depending on the circumstances of the case, the controller may have immediately identified and taken action against the individual who has accessed personal data before they were able to do

[424] Section III.C, p. 21; see there for further guidance on the alternative ways to communicate a data breach to affected data subjects.
[425] *Idem*, pp. 21 – 22.
[426] Section III.D, p. 22.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

anything with it. Due regard still needs to be given to the possible consequences of any breach of confidentiality, again, depending on the nature of the data concerned.

- It would involve disproportionate effort to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. For example, the warehouse of a statistical office has flooded and the documents containing personal data were stored only in paper form. Instead, the controller must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner. In the case of disproportionate effort, technical arrangements could also be envisaged to make information about the breach available on demand, which could prove useful to those individuals who may be affected by a breach, but the controller cannot otherwise contact.

In accordance with the accountability principle controllers should be able to demonstrate to the supervisory authority that they meet one or more of these conditions. It should be borne in mind that while notification may initially not be required if there is no risk to the rights and freedoms of natural persons, this may change over time and the risk would have to be re-evaluated.

If a controller decides not to communicate a breach to the individual, Article 34(4) explains that the supervisory authority can require it to do so, if it considers the breach is likely to result in a high risk to individuals. Alternatively, it may consider that the conditions in Article 34(3) have been met in which case notification to individuals is not required. If the supervisory authority determines that the decision not to notify data subjects is not well founded, it may consider employing its available powers and sanctions.

Assessing risk and high risk:

Once again, it may suffice to quote the WP29 Guidelines:[427]

Although the GDPR introduces the obligation to notify a breach, it is not a requirement to do so in all circumstances:

- Notification to the competent supervisory authority is required unless a breach is unlikely to result in a risk to the rights and freedoms of individuals.
- Communication of a breach to the individual is only triggered where it is likely to result in a high risk to their rights and freedoms.

This means that immediately upon becoming aware of a breach, it is vitally important that the controller should not only seek to contain the incident but it should also assess the risk that could result from it. There are two important reasons for this: firstly, knowing the likelihood and the potential severity of the impact on the individual will help the controller to take effective steps to contain and address the breach; secondly, it will help it to determine whether notification is required to the supervisory authority and, if necessary, to the individuals concerned.

As explained above, notification of a breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals, and the key trigger requiring communication of a breach to data subjects is where it is likely to result in a high risk to the rights and freedoms of individuals. This risk exists when the breach may lead to

[427] Section IV.A and B, p. 23, references omitted; again somewhat edited for presentation purposes.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

physical, material or non-material damage for the individuals whose data have been breached.

Examples:

Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur.

Factors to consider when assessing risk

Recitals 75 and 76 of the GDPR suggest that generally when assessing risk, consideration should be given to both the likelihood and severity of the risk to the rights and freedoms of data subjects. It further states that risk should be evaluated on the basis of an objective assessment.

It should be noted that assessing the risk to people's rights and freedoms as a result of a breach has a different focus to the risk considered in a DPIA)40. The DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach. When considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue; in other words, it is an assessment of a hypothetical event. With an actual breach, the event has already occurred, and so the focus is wholly about the resulting risk of the impact of the breach on individuals.

Example:

A DPIA suggests that the proposed use of a particular security software product to protect personal data is a suitable measure to ensure a level of security appropriate to the risk the processing would otherwise present to individuals. However, if a vulnerability becomes subsequently known, this would change the software's suitability to contain the risk to the personal data protected and so it would need to be re-assessed as part of an ongoing DPIA.

A vulnerability in the product is later exploited and a breach occurs. The controller should assess the specific circumstances of the breach, the data affected, and the potential level of impact on individuals, as well as how likely this risk will materialise.

Accordingly, when assessing the risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring. WP29 therefore recommends the assessment should take into account the following criteria:[428]

The type of breach

The type of breach that has occurred may affect the level of risk presented to individuals.

[428] Article 3.2 of Regulation 611/2013 provides guidance the factors that should be taken into consideration in relation to the notification of breaches in the electronic communication services sector, which may be useful in the context of notification under the GDPR. See: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF [original footnote]

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Example:

A confidentiality breach whereby medical information has been disclosed to unauthorised parties may have a different set of consequences for an individual to a breach where an individual's medical details have been lost, and are no longer available.

The nature, sensitivity, and volume of personal data

Of course, when assessing risk, a key factor is the type and sensitivity of personal data that has been compromised by the breach. Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to other personal data that may already be available about the data subject. For example, the disclosure of the name and address of an individual in ordinary circumstances is unlikely to cause substantial damage. However, if the name and address of an adoptive parent is disclosed to a birth parent, the consequences could be very severe for both the adoptive parent and child.

Breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft. A combination of personal data is typically more sensitive than a single piece of personal data.

Some types of personal data may seem at first relatively innocuous, however, what that data may reveal about the affected individual should be carefully considered. A list of customers accepting regular deliveries may not be particularly sensitive, but the same data about customers who have requested that their deliveries be stopped while on holiday would be useful information to criminals.

Similarly, a small amount of highly sensitive personal data can have a high impact on an individual, and a large range of details can reveal a greater range of information about that individual. Also, a breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals.

Ease of identification of individuals

An important factor to consider is how easy it will be for a party who has access to compromised personal data to identify specific individuals, or match the data with other information to identify individuals. Depending on the circumstances, identification could be possible directly from the personal data breached with no special research needed to discover the individual's identity, or it may be extremely difficult to match personal data to a particular individual, but it could still be possible under certain conditions. Identification may be directly or indirectly possible from the breached data, but it may also depend on the specific context of the breach, and public availability of related personal details. This may be more relevant for confidentiality and availability breaches.

As stated above, personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without the decryption key. Additionally, appropriately-implemented pseudonymisation (defined in Article 4(5) as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person") can also reduce the likelihood of individuals

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

being identified in the event of a breach. However, pseudonymisation techniques alone cannot be regarded as making the data unintelligible.

Severity of consequences for individuals.

Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm.

Whether the controller is aware that personal data is in the hands of people whose intentions are unknown or possibly malicious can have a bearing on the level of potential risk. There may be a confidentiality breach, whereby personal data is disclosed to a third party, as defined in Article 4(10), or other recipient in error. This may occur, for example, where personal data is sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. In both cases, given that the controller has an ongoing relationship with them, and it may be aware of their procedures, history and other relevant details, the recipient may be considered "trusted". In other words, the controller may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the controller promptly and to co-operate with its recovery. In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals. Again, this will depend on case-by-case basis. Nevertheless, the controller still has to keep information concerning the breach as part of the general duty to maintain records of breaches (…).

Consideration should also be given to the permanence of the consequences for individuals, where the impact may be viewed as greater if the effects are long-term.

Special characteristics of the individual

A breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result. There may be other factors about the individual that may affect the level of impact of the breach on them.

Special characteristics of the data controller

The nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach. For example, a medical organisation will process special categories of personal data, meaning that there is a greater threat to individuals if their personal data is breached, compared with a mailing list of a newspaper.

The number of affected individuals

A breach may affect only one or a few individuals or several thousand, if not many more. Generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

individual, depending on the nature of the personal data and the context in which it has been compromised. Again, the key is to consider the likelihood and severity of the impact on those affected.

General points

Therefore, when assessing the risk that is likely to result from a breach, the controller should consider a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. Clearly, where the consequences of a breach are more severe, the risk is higher and similarly where the likelihood of these occurring is greater, the risk is also heightened. If in doubt, the controller should err on the side of caution and notify. Annex B provides some useful examples of different types of breaches involving risk or high risk to individuals.

The European Union Agency for Network and Information Security (ENISA) has produced recommendations for a methodology of assessing the severity of a breach, which controllers and processors may find useful when designing their breach management response plan.[429]

- o – O – o -

[429] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity [original footnote]

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Attachment:

Examples of personal data breaches and who to notify (From the WP29 Guidelines)

Example	Notify the supervisory authority?	Notify the data subject?	Notes/recommendations
i. A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No.	No.	As long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However if it is later compromised, notification is required.
ii. A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals are exfiltrated. The controller has customers in a single Member State.	Yes, report to the supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	
iii. A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records	No.	No.	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
iv. A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.		other likely consequences.	availability or confidentiality. However, if the supervisory authority became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.
v. An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.	Yes.	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.
vi. A controller operates an online marketplace and has customers in multiple Member States. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	Yes, report to lead supervisory authority if involves cross-border processing.	Yes, as could lead to high risk.	The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk. The controller should also consider any other notification obligations, e.g. under the NIS Directive as a digital service provider.
vii. A website hosting company acting as a	As the processor, the website hosting	If there is likely no high risk to the	The website hosting company (processor)

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

data processor identifies an error in the code which controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.	company must notify its affected clients (the controllers) without undue delay. Assuming that the website hosting company has conducted its own investigation the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having "become aware" once they have been notified by the hosting company (the processor). The controller then must notify the supervisory authority.	individuals they do not need to be notified.	must consider any other notification obligations (e.g. under the NIS Directive as a digital service provider). If there is no evidence of this vulnerability being exploited with any of its controllers a notifiable breach may not have occurred but it is likely to be recordable or be a matter of non-compliance under Article 32.
viii. Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	
ix. Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
x. A direct marketing e-mail is sent to recipients in the "to:" or "cc:" fields, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist) or if other factors present	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

	high risks (e.g. the mail contains the initial passwords).		

- o – O – o -

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

TASK 7: Investigation task (including the handling of both internal and external complaints)

Note: This task is separate and distinct from the handling of data subjects' requests for access, correction, etc., as addressed in Task 8.

Investigation

Although this is not explicitly mentioned in the GDPR, it follows from the broad descriptions of the DPO's overall position and tasks – and in particular from her duty to "monitor compliance" with the GDPR: Art. 39(1)(b) – that the DPO may, on her own initiative or at the request of management or, e.g., of the staff representative body or trade union, or indeed of any individual (from within or without the organisation, or even a whistleblower, who is hopefully protected in the country concerned) **investigate** matters and occurrences directly relating to her tasks and **report** back to the person or body who commissioned or requested the investigation and/or to top management. As the EDPS puts it in his Position Paper on DPOs:[430]

> **Monitoring of compliance**(…): the DPO is to ensure the application of the Regulation within the institution. The DPO may, on his own initiative or at the request of the institution or body, the controller, the staff committee or any individual investigate matters and occurrences directly relating to his/her tasks and report back to the person who commissioned the investigation or to the controller.

The GDPR makes clear – albeit in less explicit terms than the *Annex* to the EU institutional data protection regulation – that DPOs must be given **all relevant resources** and **access to all data and premises, data-processing installations and data carriers** (with all relevant and necessary ***authentication*** and ***log access and retention*** powers) needed to carry out her tasks (cf. Art. 38(2)), i.e., also in relation to such investigations.[431] Similarly, although again this is stated more explicitly in relation to EU institutional DPOs than to DPOs appointed under the GDPR, **all of the relevant controller's staff – and indeed any external agencies' staff, including in particular processors (including cloud service providers used by the controller) – should fully assist the DPO in any such investigations**, and give ***full answersand information*** in response to any questions or requests from the DPO.[432]**Controllers should make this explicitly clear in internal staff guidance, and include clear clauses to this effect in their contracts with external providers and processors.**

Enforcement

Despite having competence to monitor compliance with the GDPR, to handle complaints, and to investigate possible breaches of the Regulation, **the DPO has limited powers of enforcement**. In principle, as noted, above, if the DPO finds that the GDPR has in some respect not been complied with by her organisation, or by any external provider or processor, the DPO should report this to senior management – and it is then the

---

[430] EDPS, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001 (footnote 243, above), p.6, original emphasis in bold.

[431] The *Annex* to Regulation (EU) 45/2001 stipulates that EU institutional DPOs: "*shall have access at all times to the data forming the subject-matter of processing operations and to all offices, data-processing installations and data carriers.*" (*Annex*, article 4, second sentence).

[432] The *Annex* to Regulation (EU) 45/2001 stipulates that: "*Every controller concerned shall be required to assist the Data Protection Officer in performing his or her duties and to give information in reply to questions*." (*Annex*, Art. 4, first sentence).

responsibility of senior management to take corrective action including, where appropriate, sanctions against any staff or agents or processors that have failed in their relevant duties, e.g., by issuing warnings or other penalties or, in extreme cases, dismissal or termination of contracts. For instance, if an outside service provider is used to collect data (e.g., through automated systems operated by the provider), and that provider does not comply with the GDPR, e.g., in terms of information notices or, worse, by using the collected data surreptitiously for further (undeclared) purposes, the DPO should propose that the controller uses another provider, and at the same time alert the DPA.

Failure to take such action will count against the controller (the organisation) in the consideration of enforcement action by the state data protection authority (DPA), including in setting the level of any "administrative fine" that may be imposed (cf. Art. 83).

Moreover, one of the tasks of the DPO is to "consult" the relevant DPA "where appropriate", with regard to any matter arising (Art. 39(1)(e)). In case of a serious difference of views between the DPO and her organisation's top management, when it is the view of the DPO that a particular processing operation is or will be in (significant) breach of the GDPR and/or relevant national law, but which management still wants to undertake, or against which it intends to take no sanction, it would certainly seem to be "appropriate" for the DPO to exercise this power and (effectively) refer the matter to the DPA. It will then be up to the DPA to use its – strong – investigative- and enforcement powers, including the possibility to order the non-implementation or stopping of the operation, as it (the DPA) deems appropriate (see Art. 58(2)(d) and (f) in particular).

See further below, under the headings "*Cooperation with and consultation of the DPA*" and "*Handling queries and complaints*".

- o – O – o -

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Advisory tasks

TASK 8: Advisory task – general

DPOs must ensure that the Regulation is respected and advise controllers on fulfilling their obligations. The DPO may therefore **inform**, offer **advice** or make **recommendations** for the ***practical improvement*** of data protection by the organisation and/or on matters concerning the application of data protection provisions (i.e., of the GDPR and other EU data protection law – such as, for now, the 2002 e-Privacy Directive and, in future, a possible e-Privacy Regulation – and of any national aw expanding on the "specification clauses" in the GDPR or otherwise applicable); and for ***the amending and updating of the organisation's data protection policies and practices*** in the light of new legal instruments, decisions, measures or guidance (cf. Art. 39(1)(a)).

To this end, the DPO should be enabled to **closely follow legislative and regulatory developments in the areas of data protection, data security, etc.**, so as to alert senior and relevant lower management of upcoming ***new EU instruments*** (such as the e-Privacy Regulation, just mentioned) or new ***EU-level executive or judicial decisions*** (such as any relevant new "adequacy" decision by the European Commission relating to third countries to which the DPO's organisation transfers data, or relevant judgments by the CJEU); ***new EU-level guidance*** (in particular, any opinions or recommendations, etc., issued by the ***EDPB***); and ***similar instruments, decisions, measures or guidance issued in the DPO's own country*** (or countries) of establishment. The GDPR indeed **requires** every controller with a DPO to provide the DPO with "***[all] resources necessary*** *to carry out [his or her] task … and* ***to maintain his or her expert knowledge***" (Art. 38(2)). The DPO should therefore be allowed – and indeed encouraged – to attend relevant seminars, conferences and meetings, in particular any organised by the national or regional state data protection authority (or -ies).

The DPO **may also beconsulted** by management, the staff representative body or trade union, or indeed of any staff member, including of course in particular any "business owners"/persons within the organisation with specific responsibilities for a specific processing operation, whenever such a person may want advice – and indeed generally **must be consulted** on relevant matters (cf. also Task 7, discussed next).

As the WP29 put it in its Guidance on DPOs (since formally endorsed by the EDPB):[433]

> Consequently, the organisation should ensure, for example, that:
>
> - The DPO is invited to participate regularly in meetings of senior and middle management.
> - His or her presence is recommended where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice.
> - The opinion of the DPO must always be given due weight. In case of disagreement, the WP29 recommends, as good practice, to document the reasons for not following the DPO's advice.
> - The DPO must be promptly consulted once a data breach or another incident has occurred.
>
> Where appropriate, the controller or processor could develop data protection guidelines or programmes that set out when the DPO must be consulted.

[433] WP29, Guidelines on DPOs (footnote 242, above), pp. 13 – 14.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

TASK 9: Supporting and promoting "Data Protection by Design & Default"

As noted in the discussion of Task 6, above, the DPO must generally be consulted on any matter relating to data protection that arises within her organisation, including in the drafting of general policy guidelines, etc.

However, there is one matter that is of particular importance in this regard. This is the new explicit requirement of the GDPR (not yet spelled out in the 1995 Data Protection Directive, although it could already be, and was, read into that),[434] that controllers embed the principle of "**data protection by design and by default**" (which includes the principle of "***security by design [and default]***")[435] into all their operations. As it is put in Article 25:

> Article 25
>
> **Data protection by design and by default**
>
> 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
> 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
> 3. …[436]

We can only briefly discuss the principle here. The EDPS sums up the **general concept and its background** as follows:[437]

> The term "privacy by design" was originally used by Ann Cavoukian when she was the Information and Privacy Commissioner of Ontario, Canada. In her concept, privacy by

---

[434] Cf., for instance, the repeated reference to the principle in the WP29 Opinion 8/2014 on the on Recent Developments on the Internet of Things (WP223), adopted on 16 September 2014, available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[435] Cf. WP223 (previous footnote), p. 22, penultimate bullet-point.

[436] The third paragraph stipulates that: "*An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.*" This is discussed in relation to Task 9, below.

[437] EDPS, Preliminary Opinion on privacy by design (Opinion 5/2018), issued on 31 May 2018, p. 4, para. 17 (original italics),available at: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (emphases added)
Note that the EDPS distinguishes the broader principle of "privacy by design", which has a "visionary and ethical dimension", from the more specific legal "data protection by design" and "data protection by default" requirements of Article 25 GDPR: p. 1, para. 4.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

> design can be broken down into "**7 foundational principles**",[438] emphasising the need to be **proactive** in considering the privacy [or in EU terms: data protection] requirements as of the design phase throughout the entire data lifecycle, to be "*embedded into the design and architecture of IT systems and business practices...without diminishing functionality...*", with privacy as the default settings, end-to-end security including secure data destruction and strong transparency subject to independent verification. The principle of privacy by default was elicited as the second of the foundational principles, establishing that privacy by design involves "*ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — **it is built into the system, by default***". This statement, is a powerful operational definition of the principle of privacy by default, where the individual does not bear the burden of striving for protection when using a service or a product but enjoys "automatically" (no need for active behaviour) the fundamental right of privacy and personal data protection.

In the view of the EDPS, "data protection by design" has **several dimensions**; to paraphrase:[439]

- the **first dimension** is that personal data processing operations should always be the ***outcome of a design project***, covering ***the whole project lifecycle***, within which the data protection risks and requirements should be clearly identified;
- the **second dimension** is that the design project should be based on a ***risk management approach***, within which the assets to be protected are ***the individuals whose data are to be processed and in particular their fundamental rights and freedoms***;
- the **third dimension** is that the measures to be taken to protect those individuals and rights and freedoms must be ***appropriate and effective*** in relation to those risks, viewed in the light of the data protection principles set out in Article 5 GDPR, which can be seen as ***goals to achieve***;
- the **fourth dimension** is the obligation to ***integrate the identified [necessary, appropriate and effective] safeguards into the processing***.

He adds that:[440]

> **All four dimensions are equally important and become an integral part of accountability** and will be subject to supervision from the competent data protection supervisory authorities where appropriate.

The EDPS stresses the importance of data protection by design and default in relation to a variety of actors: controllers and processors generally;[441] developers of (privacy-sensitive)

---

[438] See: The "seven foundational principles" are: 1. Proactive not Reactive, Preventative not Remedial; 2. Privacy as the Default Setting; Privacy Embedded into Design; 4. Full Functionality — Positive-Sum, not Zero-Sum; 5. End-to-End Security — Full Lifecycle Protection; 6. Visibility and Transparency — Keep it Open; 7. Respect for User Privacy — Keep it User-Centric. [original footnote] https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf.

[439] For the full details of these dimensions as viewed by the EDPS, see his Preliminary Opinion 5/2018 (footnote 437, above), pp. 6 – 7 (paras. 27 – 32).

[440] *Idem*, p. 7, para. 32, emphasis in bold added.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

products and technologies;[442] e-communication services;[443] e-identity services;[444] providers of "smart" maters and grids.[445] In relation to **public administrations**, the EDPS stresses that:[446]

> Article 25 applies to all types of organisations acting as controllers, including **public administrations**, which, considering their role to serve the public good, **should give the example in protecting individuals' fundamental rights and freedoms**. The GDPR stresses the role of data protection by design and by default when public administrations need to identify their providers of products and services in Recital 78, stating the **"*The principles of data protection by design and by default should also be taken into consideration in the context of public tenders*".Public administration are called be in the frontline in applying these principles in an accountable way, ready to demonstrate their implementation**, if necessary, to the competent supervisory authority.

The reference to **public tenders** is especially important: DPOs should ***advise*** their organisation that in issuing such tenders, public administrations should expressly call for applicants that can "demonstrate" that their product or service fully complies with the GDPR (and other relevant EU and national data protection law),[447] and that have embedded "data protection by design and default" in the relevant product or service. It should indeed be possible to give a ***competitive advantage*** to such applicants over and above applicants with products or services that cannot be shown to meet those requirements.[448]

The EDPS discusses at some length the various **methodologies** that have been developed to implement data protection by design and default.[449] These cannot be set out here in full or even paraphrased – but DPOs should fully familiarise themselves with them (indeed, in more detail than is provided in the EDPS paper). Suffice it to note that **the EDPS rightly links privacy by design and default to data protection impact assessments (DPIAs)**, as discussed in Task 4, above);[450] and more generally that, as the EDPS also expressly stresses:[451]

> **The role of privacy and data protection officers is central and their involvement is crucial in a privacy by design approach.** They need to be in the loop from the early stages when organisations plan systems for the processing of personal data, so that they can support managers, business owners and IT and technology departments as necessary. Their skill set should match these requirements.

That "skill set" should include being **fully educated and trained in the relevant methodologies** and technologies (if needs be, by additional in-the-job training), and being

---

441 *Idem*, p. 7, paras. 35 – 36.

442 *Idem*, p. 7, para. 37.

443 *Idem*, pp. 8 – 9, paras. 42 – 44 (with reference to the e-Privacy Directive and the proposed e-Privacy Regulation).

444 *Idem*, p. 9, para. 45 (with reference to the eIDAS Regulation).

445 *Idem*, pp. 9 – 10, paras. 46 – 50 (with reference to the Smart Meter DPIA Template Recommendation).

446 *Idem*, p. 8, para. 38, original italics, emphasis in bold added.

447 See the discussion of the "accountability" principle in Part Two, section 2.4, above.

448 This approach is expressly adopted under the Schleswig-Holstein data protection law.

449 EDPS, Preliminary Opinion 5/2018 (footnote 437, above), pp. 13 – 15, paras. 63 – 72. See also the specific references to the U.S. NIST privacy engineering program and its report on privacy engineering and risk management for U.S. federal systems (p. 11, para. 56, footnotes 76 and 74) and the EU ENISA 2014 analysis of the (then) state of the art (p. 12, para. 59, footnote 82.

450 *Idem*, p. 8, paras. 39 – 40.

451 *Idem*, p. 15, para. 76, emphasis added.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

deeply involved in the design, development, testing and tuning of all privacy-sensitive products, services and actions of their organisation (including tendering, as just noticed), at all stages.

- o – O – o –

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

TASK 10: Advise on and monitoring of compliance with data protection policies, joint controller-, controller-controller and controller-processor contracts, Binding Corporate Rules and data transfer clauses

In order to comply with the GDPR, and especially in order to "demonstrate" such compliance, controllers can and should adopt or sign up to a range of measures. As noted in section 2.2.2, above, these include:

- drawing up and formally adopting internal **data protection policies** (see Art. 24(2)) to regulate matters such as:
  - ✓ the organisation's **paper forms**, **web forms** and **data protection/privacy statements on websites**, the use of **cookies** and other trackers;
  - ✓ **access and alteration logs**, etc. in relevant soft- and hardware;
  - ✓ the issuing of "**patches**" for its own software;
  - ✓ etcetera;
- adopting **administrative agreements** ("**arrangements**") between public authorities or bodies, especially if they can be said to be "**joint controllers**" over certain processing operations;
- drafting and agreeing relevant **contracts with other controllers and processors**; and
- signing up to or drafting **standard- or individually-approved data transfer contracts**.

The main point to be re-emphasised here is that these are all responsibilities ("compliance demonstration" means) of the controller rather than the DPO (see the sub-section on "*The non-responsibility of the DPO for compliance with the GDPR*", in Part Two, section 2.5.4, above).

However, in practice the DPO should again be closely involved in all these matters. At the very least, any new DPO – and especially any DPO appointed to an organisation that did not previously have a DPO – should **review** any existing documents and instruments of this kind, to see if they still fully meet all the data protection-legal requirements.

On the basis of such a review, she should **recommend changes in existing documents etc.** – especially if those were drawn up and adopted prior to the adoption and coming into force of the GDPR; and she should **recommend the drafting and adoption of such documents** etc. where (in her view) there should be such documents etc., but there are not.

And the DPO *is* formally charged with then **monitoring** compliance with any policies, arrangements and contracts adopted or entered into by the controller in relation to personal data processing (cf. Art. 39(1)(b)).

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

TASK 11: Involvement in codes of conduct and certifications

We noted in Part Two, section 2.2.2, above, that adherence to, and full compliance with, an approved **code of conduct** or an approved **data protection certification**, could also serve as important element or means to demonstrate compliance with the GDPR in relation to the matters covered in such codes or certifications (without this amounting to legal proof of compliance).

Again, it will ultimately be up to the controller – not the DPO – to decide whether to sign up to a relevant code for the sector in which the organisation operates, or whether to seek to obtain a data protection certification of the type envisaged in the Regulation (see Arts. 40 – 43). However, it would be perfectly acceptable for a DPO to **recommend** such action.

Indeed, it might be quite appropriate for DPOs of organisations operating in a certain sector to be involved in the **drafting of (a) code(s) of conduct** for that sector, although it should also involve legal counsel and staff members of the sectoral organisation under which wing the code is drafted (including especially ICT staff if the code touches on technical issues such as ICT security, encryption, etc.).

The DPO can also **assist in the obtaining of a certification** by her organisation, by helping to put together or provide, to the Certification Body in question, "all information and access to its processing activities which are necessary to conduct the certification procedure" (Art. 42(6)). However, where a certification scheme relies on an **evaluation** of the personal data processing operations of the controller by one or more***independent experts*** accredited by the relevant Certification Body (as is done in the main current scheme in the EU, the *European Privacy Seal [EuroPriSe]* scheme),[452] the DPO cannot act in that role: that would constitute a conflict of interest.

Note: To some extent, the detailed record of data protection impact assessments (DPIAs), discussed in Task 4, above, and the continued monitoring of operations, discussed in Task 5, above (and the records of that continuous monitoring) fulfil a similar function to certifications, in that these records show that the controller and its staff have carefully looked at all the privacy/data protection implications of the relevant personal data processing operations; have identified and quantified the risks involved to the fundamental rights of the individuals affected; and have adopted appropriate mitigating measures. The advantage of certifications over this is that the evaluation is done by outside, independent experts. However, much will depend on the quality of the accredited certification schemes and on how they will inter-relate to enforcement by the DPAs.

- o – O – o -

[452] See: https://www.european-privacy-seal.eu/EPS-en/fact-sheet

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Cooperation with and consultation of the DPA

TASK 12: Cooperation with the DPA

The DPO has the task of responding to requests from the DPA and, within the sphere of her competence, cooperate with the DPA at the latter's request or on his/her own initiative (Art. 39(1)(d)).

In this regard, the WP29 said that:[453]

> These tasks refer to the role of 'facilitator' of the DPO mentioned in the introduction to these Guidelines. The DPO acts as a contact point to facilitate access by the supervisory authority to the documents and information for the performance of the tasks mentioned in Article 57, as well as for the exercise of its investigative, corrective, authorisation, and advisory powers mentioned in Article 58. As already mentioned, the DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law (Article 38(5)). However, the obligation of secrecy/confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority. Article 39(1)(e) provides that the DPO can consult the supervisory authority on any other matter, where appropriate.

The EDPS has very usefully expanded further on the equivalent duties of the EU institutional DPOs, in their relations with the EDPS, as set out in the quotes below with textual amendments to apply the EDPS's words, *mutatis mutandis*, to the relationship between the Member States' data protection authorities (DPAs) (and the EDPB) and DPOs appointed under the GDPR. He first of all notes, in general terms, that:[454]

> The DPO has the task of responding to requests from the [relevant data protection authority] and, within the sphere of his competence, cooperate with the [DPA] at the latter's request or on his/her own initiative. This task emphasises the fact that the DPO facilitates cooperation between the [DPA] and the institution notably in the frame of investigations, complaint handling or prior checks. The DPO not only has inside knowledge of the institution, but is also likely to know who the best person to contact within the institution is. The DPO may also be aware, and duly inform the [DPA], of recent developments likely to impact the protection of personal data.

The EDPS then elaborates on this in regard to the various matters mentioned in terms that largely also apply to the issues under the GDPR, as follows:[455]

> **IV. Relation DPO – [DPA]**
>
> Ensuring compliance with the Regulation will be influenced by the working relationship between the DPO and the [relevant DPA]. The DPO must not be seen as an agent of the [DPA], but as a part of the institution/body in which he/she works. As already mentioned, this idea of proximity puts him/her in an ideal situation to ensure compliance from the inside and to advise or to intervene at an early stage thereby avoiding possible intervention from the supervisory body. At the same time the [DPA] can offer valuable support to DPOs in the performance of their function.[456]

---

453 WP29, Guidelines on DPOs (footnote 242, above), p. 18.

454 EDPS, Position paper on DPOs (footnote 243, above),p. 6. Textual changes in square brackets.

455 *Idem*, Part IV (pp. 10 – 11).

456 Cf. the provision by the **French** data protection authority, the CNIL, of a special "*extranet*" for registered DPOs, accessible only to them with a username and password, which provides them with legal texts (laws, decrees, etc.) and training and information, including information on new reports or guidance issued by

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

The [DPAs can be expected to][457] therefore support[] the idea of developing possible synergies between DPOs and the [DPAs] which would contribute to achieving the overall aim of effective protection of personal data within the institutions.…

IV. 1. Ensuring compliance

Ensuring compliance notably starts by raising awareness. As mentioned above, DPOs play an important role in developing knowledge on data protection issues inside the institution/body. The [DPAs can be expected to][458] welcomes this and its consequence in terms of stimulating an efficient preventive approach rather than repressive data protection supervision.

The DPO also provides advice to the institution/body on practical recommendations for improvement of data protection within the institution/body or concerning the interpretation or application of the [GDPR].[459] This advisory function is shared with the [DPAs] who shall advise all [their domestic] institutions/bodies on matters concerning the processing of personal data ([Article 57(1)(c) GDPR])). In this field the [national DPOs have already in the past] often been called upon to advise DPOs on specific issues related to data protection (case by case approach). The [DPAs and the EDPB can be expected] to produce position papers on certain themes so as to afford guidance to the institutions/bodies on certain more general topics.[460]

IV.2 Prior checks

Opinions delivered [by a DPA] in the framework of an [Article 36 GDPR prior consultation] [and views expressed by DPAs in the process of issuing prior authorisations as envisaged in Article 36(5) GDPR], are also the occasion for the [DPA] to monitor and ensure compliance with the [GDPR]. …[461]

… [B]efore the final adoption of a prior check opinion, the [DPA may][462]send[] a provisional draft to the DPO with information on intended recommendations thereby opening up room for discussion on efficiency and consequences of intended

---

the CNIL, and on other legal and practical developments, and allows them to exchange views and hold discussions. See section 2.3.5, under the heading "*Formal training and certification*" and footnote 274, above.

457 The original sentence says the EDPS "supports" the idea. The DPAs (and the EDPB) can be expected to take the same view.

458 The original sentence says the EDPS "welcomes" this approach, but (also in the light of past practice) the DPAs (and the EDPB) can again be expected to take the same view.

459 The reference in the EDPS paper is to the regulation setting out the data protection rules for the EU institutions themselves (Regulation (EC) 45/2001) (footnote 148, above), but the same is of course true in relation to the GDPR as concerns DPOs appointed under that latter regulation. We have made similar replacements elsewhere in the quote.

460 The original sentence says the EDPS "intends to produce" position papers and guidance. Again, the national DPAs and the EDPB can be expected to do the same in relation to the GDPR.
mitted sentence reads: "" With regard to DPOs appointed under the GDPR, the national DPAs, but especially also the new EDPB, will undoubtedly issue similar guidance.

461 The remainder of this paragraph, and the omitted sentence at the beginning of the next paragraph, deal with the fact that the time gap between the entry into force of the Regulation and the appointment of the EDPS created a large backlog of cases which are being "prior checked" on an "ex post" basis. It is not clear yet if similar problems are arising under the GDPR. If so, the EDPS's call for the DPOs and the regulator to be "strategic partners" in resolving this should also be heeded in that context.

462 The practice of sending "provisional draft recommendations" to a controller in the context of a "prior consultation"/"prior authorisation" process is not specified in the GDPR (or indeed in Regulation 45/2001). However, the very fact that the GDPR refers to "prior *consultation*" strongly suggests that the DPAs will, under that instrument, take a similar approach; and this is reflected in the wording in square brackets twice added to this paragraph.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

recommendations. The [DPAs can be expected] to be attentive to the concerns of the institution as expressed by the DPO so as to work towards practicable recommendations.

IV. 3. Enforcement

In the area of implementation of particular data protection measures, synergy potentials between the DPOs and [DPAs] emerge as regards the adoption of sanctions and handling of complaints and queries.

As already mentioned, the DPOs have limited powers of enforcement. The [DPA] will contribute to ensuring compliance with the [GDPR] by taking effective measures in the field of prior [consultations or authorisations] and of complaints and other inquiries. Measures are effective if well targeted and feasible: the DPO can also be seen as a strategic partner in determining the well targeted application of a measure.

The handling of complaints and queries by the DPO at a local level[463] is to be encouraged at least as concerns a first phase of investigation and resolution. The [DPAs may][464] therefore [be expected to take the view] that DPOs should try to investigate and resolve complaints at a local level before referring to the [DPA]. The DPO should also … consult the [DPA] whenever he/she has doubts on the procedure or content of complaints. This does not however prevent the data subject from addressing him/herself directly to the [DPA] under [Article 77(1) GDPR]. The limited powers of enforcement of the DPO also imply that in some cases, the complaint or query must be escalated to the [DPA]. The [DPA] therefore provides for valuable support in the field of enforcement. In turn, the DPO can be relied on to provide information to the [DPA] and to provide follow-up on the measures adopted.

IV.4. Measuring effectiveness[465]

As concerns measuring the effectiveness of the implementation of the data protection requirements, the DPO must be seen as a useful partner to evaluate progress in this area. For example, when it comes to measuring performance of internal data protection supervision, the [DPAs can be expected to] encourage[] DPOs to develop their own criteria of good supervision (professional standards, specific plans for the institution, annual work programme...). These criteria will in turn enable the [DPA], where invited to do so, to evaluate the work of the DPO, but will also serve to enable him to measure the state of implementation of the [GDPR] within the institution/body.

It is also likely that DPOs in the public sector will be called upon by their DPAs to contribute to consultations held by the DPAs, and to provide input when a DPA is

[463] Note that the handling of requests and complains from data subjects is further discussed in Task 11, below.

[464] The first two sentences in this paragraph again refer to EDPS-promoted practice – but it is again (also in view of past practice) fully to be expected that the national DPAs will take the same approach (as indicated in the wording in square brackets).

[465] There are no specific requirements, either in Regulation 45/2001 (with regard to the EU institutions), or in the GDPR (with regard to entities covered by that instrument), for the relevant regulator (respectively, the EDPS and the national DPAs) to "measure the effectiveness" of the measures adopted by controllers with the aim of ensuring compliance with the applicable instrument. Within the EU institutional framework, the EDPS does however (rightly) view this a natural part of his job. It is to be expected that the Member States' DPAs (and the EDPB) will also "encourage" DPOs to contribute to high-level compliance through the adoption or adhesion of "professional standards, specific plans for the institution, annual work programme", etc.; as is again reflected in the wording in square brackets.

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

preparing a formal opinion on proposed or draft laws in the area of data protection that touches on the context within which the DPO operates.

Finally, it should be noted that **the DPO plays an important role in helping the DPA in its carrying out on-the-spot inspections**, in DPO consultations with controllers in specific sectors, etc. For instance, it is rare for DPAs to carry out inspections without notice – this is really only done in relation to suspected miscreants who may hide data or other evidence if given prior warning of an inspection. In practice, DPAs normally pre-arrange inspections with the help of the controller, and in particular the controller's DPO, who will be able to ensure that the right people are available and the right places and systems can be inspected. This is often crucial, especially in relation to complex processing systems where in-depth knowledge of the ICT architecture and internal processes is required for a proper review. And when a DPA wants to examine in detail the processing of personal data in a particular context or sector – as most of them do under an annually-determined plan and selection of priorities – they will turn to the DPOs of controllers active in the context or sector for real insight, holding meetings with them and asking for responses to consultations. This too is part of what the EDPS calls the "strategic partnership" between DPOs and DPAs.

- o – O – o -

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Handling data subject requests

TASK 13: Handling data subject requests and complaints

The GDPR stipulates that:

> Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.
>
> (Art. 38(4))

Data subjects who want to exercise any of their **data subject rights** – rights of access, rectification and erasure ("right to be forgotten"), restriction of processing, data portability, right to object in general and in relation to automated decision-making and profiling – in respect of an organisation, or who have **general questions** or data protection-related **complaints** about the organisation, should therefore normally address themselves first of all to the DPO of that organisation (where there is one).

This is facilitated by the requirement in the GDPR that the contact details of the DPO must be published by the organisation (Art. 37(7)) and that the controller must ensure "*that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data [relating to the organisation]*" (Art. 38(1)). (Therefore, if a data subject were to address her- or himself to someone else in the organisation, such as the general counsel or the CEO, those should pass on the request to the DPO.)

Moreover, the independent status of the DPO (Art. 38(3)) should ensure that the request, query or complaint is handled by the DPO – or by the responsible staff members under the supervision of the DPO – in an **appropriate manner, without bias in favour of the organisation or against the data subject**. In any case, the DPO should either herself write, or review, the response to the data subject. This should include the advice that, if the data subject is not content with the response, he or she can raise the issue with the DPA.

This is because, in any case, the data subjects' right to submit requests, queries and complaints to the organisation (i.e., to the organisation's DPO) is **without prejudice to their right to complain to the DPA**. Specifically, each DPA is required and empowers, on its own territory, to:

> handle complaints lodged by a data subject … and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation …
>
> (Art. 57(1)(f))

In such complaints to the DPA, data subjects can be represented by a relevant not-for-profit body (Art. 80), and the above duty and power of the DPA to handle such complaints extends to cases brought in this way (see the words in Article 57(1)(f), omitted from the above quote).

In that light, it would make sense for DPOs to also be willing to entertain requests and **complaints from such representative organisations**, rather than only from data subjects.

As already noted in relation to Task 10 (*Cooperation with the DPA*), it is to be expected (also in the light of past practice) that the national DPAs (like the EDPS in relation to the EU institutional DPOs) will encourage data subjects (and such organisations) to always first take

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

up any issues with the controller, and more specifically with the controller's DPO, to see if the matter cannot be already satisfactorily be investigated and resolved in such interactions, without involving the DPA, subject to the proviso that the DPO should consult the DPA if any questions arise about the general interpretation and application of the GDPR. But this should never go so far as to discourage data subjects (or representative organisations) from raising issues – and of course especially issues of principle – with the DPA.

As the EDPS put it, the regulator and the DPOs are in a "strategic partnership": the DPAs can encourage data subjects to first and foremost sort out any issues directly with DPOs; and DPOs must be able – and are required – to work with the regulator to make sure that responses to questions and complaints are properly handled and if needs be lead to changes in the relevant controller's practices. The DPAs must be able to rely on the DPOs to truly support data subjects in any complaint; and the DPOs must be able to rely on the DPAs to ensure that recommendations for change are actually enforced.

This reinforces the delicacy of the position of the DPO, discussed in Part Two, section 2.5: the DPOs is a bridge between the controller and regulator – and (to somewhat mix metaphors, unless one reads bridge here as gangway) should not be allowed to fall between the ship and quay.

- 0 – O – o -

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

Information and raising awareness

TASK 14: Internal and external information and awareness-raising tasks

The GDPR stipulates that the DPO's tasks shall "at least" include

> Inform[ing] and advis[ing] the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions
>
> (Art. 39(1)(a))

Internally (within the organisation where the DPO works), this implies, on the one hand, the DPO **informing** staff members of their rights and, on the other hand, the DPO **instructing** controllers and the organisation and staff members – including in particular "business owners"/persons responsible for specific operation – in their obligations and responsibilities, and **training** them in how to meet those.

As the EDPS puts it in a passage already quoted earlier:[466]

> Ensuring compliance notably starts by raising awareness. … DPOs play an important role in developing knowledge on data protection issues inside the institution/body.

Awareness-raising "stimulat[es] an efficient preventive approach rather than repressive data protection supervision".[467]

Measures adopted by the DPO towards these aims can include the issuing of **staff information notes**, the organising of internal data protection **training sessions** – which should aim to inculcate in the staff an awareness and sensibility towards data protection and data subject rights – a "data protection reflex" – in all their various roles in society, be that as an ordinary citizen, a worker, a team leader, or senior manager.

Also, the setting up of an internal data protection-informing and teaching **web site**, and the drafting and release of **privacy statements** on staff websites and -pages.[468]

Externally, apart from ensuring that data subjects are provided with relevant information when data are first collected on them (as provided for in Articles 12 – 14 GDPR), e.g. in clear website notices, the DPO should also work with any public relations staff to ensure **fulltransparencyabout the organisation's personal data processing operations**: about the purposes for which it collects and processes personal data; the categories of data subjects and data involved; the recipients of the data; whether the data are transferred to third (non-EU/EEA) countries; etc.

The GDPR does not require controllers to make the register of their personal data processing operations fully available to the public.[469] However, the GDPR also certainly does not prohibit it.

The EDPS argues strongly in favour of publication in relation to the EU institutions, in particular in the light of the fact that (like the 1995 Data Protection Directive) an earlier regulation did require them to publish their "functionally equivalent" notification details:[470]

---

466 EDPS, Position paper on DPOs (footnote 243, above), p. 10.

467 *Idem*.

468 *Idem*, p. 5.

469 By contrast, the 1995 Data Protection Directive did require the DPAs to make the details of the processing operations notified to them publicly available (Art. 21).

> Records are an important tool for checking and documenting that your organisation is in control of its processing activities. ….
>
> **The EDPS strongly recommends that [EU Institutions] make records publicly accessible, preferably through publication on the internet … .**
>
> There are many reasons why the register of records should be public:
>
> - it contributes to the transparency of EUIs12;
> - it helps to strengthen public trust;
> - it makes knowledge-sharing between EUIs easier;
> - not publishing it would be a step back behind the old [rules].

Very much the same can be said in relation to the register of processing operations to be maintained by controllers under the GDPR – at the least, as far as public authorities are concerned. Some Member States may in their national law impose such a duty to publish the details of the register; but public authorities in countries where this is not compulsory should still always consider doing so in the light of the EDPS's observations.

Of course, controllers and processors should not feel obliged to publish information on their security arrangements that could be used to breach that security (this was already recognised in the 1995 Data Protection Directive's provision on the publication of details of processing operations that had been notified to DPAs).[471]

Basic information on the organisation's personal data processing operations should in any case be easily accessible on the organisation's **website**, and also provided in **booklets** and **forms** (including versions accessible to disabled people).

The website and such forms should also clearly provide information about **how data subjects can exercise their rights** (including a clear public notice with the **contact details of the DPO** – although that does not need to include a name); what **codes of conduct** the organisation has signed up and what **certifications** it has obtained (these matters can be shown through recognised **logos** or **seals**); etcetera.

Any website should of course also fully meet the requirements of EU data protection law, and any relevant further national law, on matters such as **cookies** and other **trackers**, etc.

---

[470] EDPS, Accountability on the ground (footnote 353, above), p. 8, original emphasis.

[471] See again Article 21 of the 1995 Data protection Directive, which excludes the information listed in Article 19(1)(f) – i.e., a general description of the controller's security measures – from the information to be made publicly available. Note however that the belief in "security through obscurity" has long since been discredited, see: https://en.wikipedia.org/wiki/Security_through_obscurity

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723

TASK 15: Planning and reviewing the DPO's activities

Finally, given the vast numbers and scope of the DPO's tasks, he or she should prepare an annual plan of his or her activities, taking into account the expected time needed to perform each of them and to devote to foreseeable new developments, while also allowing for time to be given to unforeseen events; and to regularly revise and up-date this plan.

- o – O – o -

Douwe Korff & Marie Georges, Cambridge/Paris, December 2018/June 2019

(cc) Douwe Korff & Marie Georges/Final Text as approved – 190723