

OXFORD
UNIVERSITY PRESS

Compilation from

**The EU General Data Protection Regulation: A
Commentary (2nd edition)**

Forthcoming from Oxford University Press

edited by

**Christopher Kuner
Lee A. Bygrave
Christopher Docksey**

Assistant editors

**Laura Drechsler
Luca Tosoni**

Editorial assistant

Charlotte Somers

Covering developments until 31 January 2025

March 2025

Forthcoming in 2026 from Oxford University Press

The following compilation includes a selection of non-final draft commentaries on seven articles of the GDPR. The texts are working versions that are not identical with the final published versions. It is released with consent of the publisher and the authors. Please do not cite these working drafts.

LIST OF ARTICLES

Article	Topic	Author	Page
4(16)	Main establishment	Dr. Luca Tosoni, Schjødt law firm, Oslo	5
10	Processing of personal data relating to criminal convictions and offences	Dr. Teresa Quintel,* Administrator at the European Parliament Committee on Civil Liberties, Justice and Home Affairs	23
17	Right to erasure ('right to be forgotten')	Prof. Dr. Herke Kranenborg,* Legal Service of the European Commission and University of Maastricht	39
32	Security of processing	Prof. Dr. Lee Bygrave, Norwegian Research Center for Computers and Law, Department of Private Law, University of Oslo	57
45	Transfers on the basis of an adequacy decision	Prof. Dr. Christopher Kuner, University of Copenhagen and Wilson Sonsini Goodrich & Rosati, Brussels and Prof. Dr. Laura Drechsler, KU Leuven, Open Universiteit and Belgian State Archives	79
61	Mutual assistance	Christopher Docksey, Hon. Director-General EDPS, Guernsey Data Protection Authority, and University of Maastricht	115
89	Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes	Prof. Dr. Laura Drechsler, KU Leuven, Open Universiteit and Belgian State Archives and Charlotte Somers, KU Leuven	135

* The views and opinions expressed are solely those of the authors and do not necessarily reflect the official policy or position of the European Parliament or the European Commission.

Article 4(16). Main establishment

LUCA TOSONI

‘main establishment’ means:

- (a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
- (b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

Relevant Recitals

(22) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

(36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings,

the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

CLOSELY RELATED PROVISIONS

Article 4(7) (Definition of ‘controller’); Article 4(8) (Definition of ‘processor’); Article 4(19) (Definition of ‘group of undertakings’); Article 56 (Competence of the lead supervisory authority) (see too recitals 124–128); Article 60 (Cooperation between the lead supervisory authority and the other supervisory authorities concerned) (see too recitals 130–131); Article 65 (Dispute resolution by the Board)

RELEVANT CASE LAW

CJEU

Case C-81/87, *The Queen v Treasury and Commissioners of Inland Revenue, ex parte Daily Mail and General Trust plc*, judgment of 27 September 1988 (ECLI:EU:C:1988:456).

Opinion of Advocate General Darmon in Case C-81/87, *The Queen v Treasury and Commissioners of Inland Revenue, ex parte Daily Mail and General Trust plc*, delivered on 7 June 1988 (ECLI:EU:C:1988:286).

Case C-210/06, *Cartesio Oktató és Szolgáltató bt*, judgment of 16 December 2008 (Grand Chamber) (ECLI:EU:C:2008:723).

Case C-131/12, *Google Spain v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, judgment of 13 May 2014 (Grand Chamber) (ECLI:EU:C:2014:317).

Case C-230/14, *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, judgment of 1 October 2015 (ECLI:EU:C:2015:639).

Case C-191/15, *Verein für Konsumenteninformation v Amazon EU Sàrl*, judgment of 28 July 2016 (ECLI:EU:C:2016:612).

Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, judgment of 5 June 2018 (Grand Chamber) (ECLI:EU:C:2018:388).

Opinion of Advocate General Bot in Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, delivered on 24 October 2017 (ECLI:EU:C:2017:796).

Case C-617/15, *Hummel Holding A/S v Nike Inc. and Nike Retail B.V.*, judgment of 18 May 2017 (ECLI:EU:C:2017:390).

Opinion of Advocate General Tanchev in Case C-617/15, *Hummel Holding A/S v Nike Inc. and Nike Retail B.V.*, delivered on 12 January 2017 (ECLI:EU:C:2017:13).

Opinion of Advocate General Szpunar in Case C-673/17, *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände—Verbraucherzentrale Bundesverband e.V.*, delivered on 21 March 2019 (ECLI:EU:C:2019:246).

Opinion of Advocate General Bobek in Case C-645/19, *Facebook Ireland Limited, Facebook Inc., Facebook Belgium BVBA v Gegevensbeschermingsautoriteit*, delivered on 13 January 2021 (ECLI:EU:C:2021:5).

Case C-645/19, *Facebook Ireland Limited, Facebook Inc., Facebook Belgium BVBA v Gegevensbeschermingsautoriteit*, judgment of 15 June 2021 (ECLI:EU:C:2021:483).

France

French Council of State (*Conseil d’État*), *Google LLC/CNIL*, 19 June 2020, N° 430810 (ECLI:FR:CEORD:2020:440916.20200619).

French Council of State (*Conseil d’État*), *Google LLC et Google Ireland Limited/CNIL*, 4 March 2021, N° 449212 (ECLI:FR:CEORD:2021:449212.20210304).

Germany

German Federal Court of Justice (*Bundesgerichtshof*), judgment XII ZB 114/06 of 27 June 2007.

United Kingdom

Court of Appeal (England and Wales), *Young v Anglo American South Africa Limited* [2014] EWCA Civ 1130.

A. Rationale and Policy Underpinnings

The definition of ‘main establishment’ in Article 4(16) GDPR is primarily intended to determine which national supervisory authority should be the ‘lead supervisory authority’ for the purposes of a given processing operation,¹ where the controller or processor has establishments in multiple EU/EEA countries.² Article 56 GDPR terms as ‘lead supervisory authority’ the authority with the chief responsibility for dealing with a given cross-border data processing activity in accordance with the ‘one-stop-shop’ mechanism.³ The latter is an enforcement scheme intended to ensure that controllers and processors with multiple EU/EEA establishments, or whose activities substantially affect data subjects in several EU/EEA countries, have one single supervisory authority as their sole interlocutor with respect to cross-border data protection compliance matters. The ‘one-stop-shop’ mechanism was introduced to help remedy the legal uncertainty and costs linked with the inconsistent enforcement of EU data protection rules across borders. These problems were often cited among the principal shortcomings of the DPD.⁴

The concept of ‘main establishment’ constitutes the cornerstone on which the ‘one-stop-shop’ mechanism is built.⁵ Indeed, if there is no ‘main establishment’ (or single establishment where the processing substantially affects or is likely to substantially affect data subjects in more than one Member State) in the EU/EEA, the mechanism does not apply.⁶

In light of the above, the EDPB noted that:

[C]orrect identification of the main establishment is in the interests of controllers and processors because it provides clarity in terms of which supervisory authority they have to deal with in respect of their various compliance duties under the GDPR. These may include, where relevant, designating a data protection officer or consulting for a risky processing activity that the controller cannot mitigate by reasonable means. The relevant provisions of the GDPR are intended to make these compliance tasks manageable.⁷

¹ Case C-645/19, *Facebook Ireland and Others* (AG Opinion), para. 144.

² See WP29 2012, p. 16.

³ Advocate General Bot described the GDPR’s one-stop-shop mechanism as a scheme according to which ‘a controller that carries out cross-border data processing, such as Facebook, will have only one supervisory authority as interlocutor, namely the lead supervisory authority, which will be the authority for the place where the controller’s main establishment is located’: see Case C-210/16, *Wirtschaftsakademie* (AG Opinion), para. 103. See also WP29 2017, p. 4 (noting that the ‘lead supervisory authority’ is ‘the authority with the primary responsibility for dealing with a cross-border data processing activity’). See further the commentaries on Arts. 56 and 60 in this edition.

⁴ See e.g. EC Staff Working Paper 2012, p. 36.

⁵ See also WP29 2012, p. 11 (noting that ‘[a] clear understanding of the term “main establishment” is crucial, as it is decisive for determining the lead authority . . . where processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State’).

⁶ The EDPB opined that ‘controllers without any establishment in the EU must deal with local supervisory authorities in every Member State they are active in, through their local representative’. See EDPB 2023, para. 49.

⁷ *Ibid.*, para. 21.

B. Legal background

1. EU legislation

The DPD did not use the term ‘main establishment’ or similar terms. However, the DPD referred to the concept of ‘establishment’ as a criterion to identify the national law(s) applicable to the processing of personal data (Article 4(1)(a) and recital 19 DPD), and indirectly to determine which supervisory authority or authorities was/were competent under Article 28(1) DPD to apply the relevant national data protection rules to that processing. Nonetheless, the DPD did not lay down any criterion of priority governing the intervention of one supervisory authority as against another in cases where a controller was established on the territory of multiple EU/EEA countries.

The concept of ‘place of central administration’ — i.e. a key component of the definition of ‘main establishment’ in Article 4(16) GDPR — was also absent in the DPD. It is, however, found in Article 54 of the Treaty on the Functioning of the European Union (‘TFEU’) and in several other EU Regulations.⁸

2. International instruments

The concept of ‘main establishment’ is not found in Convention 108, either in its original or modernised version. The same applies with respect to the OECD Privacy Guidelines (both original and revised versions) and the APEC Privacy Framework.

3. National developments

Some national data protection laws establish specific arrangements to align their national systems with the GDPR’s ‘one-stop-shop’ mechanism, including by laying down rules to identify the competent local supervisory authority based on the location of the controller’s or processor’s ‘main establishment’. For example, section 19 of the German GDPR Implementation Law provides that:

[T]he lead supervisory authority of a *Land* in the one-stop-shop mechanism pursuant to Chapter VII of Regulation (EU) 2016/679 shall be the supervisory authority of the *Land* in which the controller or processor has its main establishment, as referred to in Article 4 no. 16 of Regulation (EU) 2016/679 or its single establishment in the European Union, as referred to in Article 56(1) of Regulation (EU) 2016/679...⁹

4. Case law

The CJEU has yet to interpret the definition of ‘main establishment’ under the GDPR.¹⁰ However, the Court has interpreted the concept of ‘establishment’ within the meaning of the

⁸ See e.g. Art. 19(1) Rome I Regulation; Art. 63(1)(b) Regulation 1215/2012; Art. 60(1)(b) Brussels I Regulation (repealed).

⁹ German GDPR Implementation Law.

¹⁰ However, the CJEU has ruled on the functioning of the one-stop-shop mechanism in Case C-645/19, *Facebook Ireland and Others*. In that case, Advocate General Bobek noted in passing that ‘Article 4(16)(a) of the GDPR embraces a dynamic understanding of what is considered to be the main establishment, which need not necessarily coincide with the static corporate structure of an undertaking’. See Case C-645/19, *Facebook Ireland and Others* (AG Opinion), para. 144.

DPD, as well as that of ‘place of central administration’ under other EU legal instruments. This jurisprudence is referenced in the next section.

At national level, France’s highest administrative court (*Conseil d’État*) interpreted the notion of ‘main establishment’ in a case concerning Google LLC’s appeal against an administrative fine that the French supervisory authority (‘CNIL’) had imposed on the company for several GDPR violations.¹¹ In its appeal, Google LLC (i.e., a U.S.-incorporated company) argued that the CNIL was not competent to issue the appealed fine, as the Irish subsidiary of its corporate group (i.e., Google Ireland Limited) was to be considered Google LLC’s ‘main establishment’ in the European Union within the meaning of Article 4(16) GDPR. This meant that pursuant to Article 56(1) GDPR, the Irish supervisory authority (‘DPC’) was competent to act as ‘lead supervisory authority’ with respect to the cross-border data processing activities covered by the CNIL’s fining decision.¹²

The *Conseil d’État* rejected Google LLC’s argument. However, it did so for reasons that have more to do with the Court’s reading of the facts of the case rather than due to a strict interpretation of the notion of ‘main establishment’. According to the *Conseil d’État*: ‘For identifying the competent supervisory authority, the central administration of the controller, that is to say the place of its real seat, must in principle be regarded as its main establishment.’¹³

This suggests that the ‘place of central administration’ corresponds to the real seat (*siège réel*) or operational headquarters of a company, which — as a general rule — should be regarded as its ‘main establishment’ for GDPR purposes.

The *Conseil d’État* further stated that the above general rule does not apply if ‘another [EU] establishment [of the controller] is competent to take decisions on the purposes and means of processing and has the power to have them implemented at Union level’,¹⁴ as in such case it is the latter establishment, and not the establishment of the ‘place of central administration’, that would qualify as the ‘main establishment’ under Article 4(16)(a) GDPR.

However, the *Conseil d’État* went on to note that:

In the event that a controller established outside the European Union puts in place a cross-border processing in the territory of the Union, but having neither a central administration nor an establishment with decision-making power as to its purposes and means [in the Union], the mechanism of the lead authority provided for in Article 56 of the GDPR does not apply.¹⁵

¹¹ Conseil d’État, *Google LLC/CNIL*.

¹² Ibid., para. 5. Google LLC had (unsuccessfully) raised the same argument also during the investigation conducted by the CNIL. See CNIL 2019, paras. 21-41.

¹³ Conseil d’État, *Google LLC/CNIL*, para. 4 (‘Pour la détermination de l’autorité de contrôle compétente, l’administration centrale du responsable du traitement, c’est-à-dire le lieu de son siège réel, doit en principe être regardée comme son établissement principal’).

¹⁴ Ibid., para. 4 (‘Il en va autrement si un autre de ses établissements est compétent pour prendre les décisions relatives aux finalités et aux moyens du traitement et dispose du pouvoir de les faire appliquer à l’échelle de l’Union’).

¹⁵ Ibid. (‘Dans l’hypothèse où un responsable de traitement implanté en dehors de l’Union européenne met en oeuvre un traitement transfrontalier sur le territoire de l’Union, mais qu’il n’y dispose ni d’administration centrale, ni d’établissement doté d’un pouvoir décisionnel quant à ses finalités et à ses moyens, le mécanisme de l’autorité chef de file prévu à l’article 56 du RGPD ne peut être mis en oeuvre’).

This led the *Conseil d'État* to conclude that Google Ireland Limited could not be qualified as the 'main establishment' of Google LLC because:

'On the one hand, it does not appear from the investigation that Google Ireland exercised, [on the date of the appealed fining decision], a power of direction or control over the other European subsidiaries of Google LLC such as to regard it as a central administration within the meaning of the GDPR. On the other hand, it appears from the investigation that that establishment, which in any case was not assigned new responsibilities with regard to the processing operations carried out by Google in Europe until ... after the date of the appealed fining decision, did not have until that date a decision-making power with regard to the purposes and means of the processing operations at issue, [at least] no more than any of the other European establishments.'¹⁶

Although the *Conseil d'État* and the CNIL reached the same conclusion on CNIL's competence, their reasoning seems to differ on one important point: the interpretation of the 'place of central administration' criterion under Article 4(16) GDPR.

According to the CNIL, 'to qualify as a main establishment, the establishment in question must have decision-making power *with regard to the processing of the personal data in question*' (emphasis added).¹⁷ This view has later been endorsed by the EDPB as well.¹⁸ This view implies that when a corporate group has its real seat or operational headquarters in the EU, but the decisions on its processing of personal data are taken outside of the EU, the group has no 'main establishment' in the EU for GDPR purposes.

However, the *Conseil d'État* seems to follow a different line of reasoning. The Irish company's lack of any decision-making power with regard to the processing of the personal data in question was not the only factor that led the Court to exclude that the Irish company was to be qualified as Google's 'main establishment'. The Court reached that conclusion also because the Irish company did not qualify as a 'central administration', as it did not have 'a power of direction or control over the other European subsidiaries'.¹⁹ In other words, that company could not be considered a proper European 'real seat' or operational headquarter. This is regardless of the Irish company's decision-making powers as regards the purposes and the means of the processing at issue.

In practice, the *Conseil d'État* appears to hold that two cumulative negative conditions must be met to exclude a company established outside of the EU from having a 'main establishment' in the EU: the company must have '*neither* a central administration *nor* an establishment with decision-making power as to [the] ... purposes and means [of the relevant processing]' in the EU.²⁰ The first negative condition would not be met where a company has a 'real seat' in the EU, regardless of whether such 'real seat' makes data-processing decisions. Indeed, the Court

¹⁶ Ibid., para. 5 ('D'une part, il ne résulte pas de l'instruction que la société Google Ireland exerçait, à cette date, un pouvoir de direction ou de contrôle sur les autres filiales européennes de la société Google LLC de nature à la regarder comme une administration centrale au sens du RGPD. D'autre part, il résulte de l'instruction que cet établissement, qui ne s'est en tout état de cause vu attribuer de nouvelles responsabilités s'agissant des traitements opérés par Google en Europe qu'à partir du 22 janvier 2019, soit postérieurement à la date de la sanction attaquée, ne disposait jusqu'à cette date d'aucun pouvoir décisionnel quant aux finalités et aux moyens des traitements litigieux, pas plus qu'aucun autre de ses établissements européens').

¹⁷ CNIL 2019, para. 30.

¹⁸ EDPB 2024, para. 37.

¹⁹ Conseil d'État, *Google LLC/CNIL*, para. 5.

²⁰ Ibid., para. 4 (emphasis added).

defines the concept of ‘central administration’ simply as the ‘real seat’²¹ of a company (i.e., an establishment with ‘powers of direction or control over other subsidiaries’),²² and juxtaposes such ‘real seat’ with an establishment with decision-making powers concerning the means and purposes of the processing.²³

The *Conseil d’État*’s reasoning suggests that there may be cases where a controller has a ‘main establishment’ in the EU even though the decisions on the purposes and means of a specific processing activity are taken outside the EU. Such cases would occur when a corporate group has a ‘real seat’ in the EU, which exercises a power of direction or control over other European subsidiaries, but the decisions on personal data processing are not taken in such a ‘real seat’ or in any other establishments in the EU. It should be noted though that the EDPB has rejected this view and — as outlined further on — it is of the opinion that a ‘place of central administration’ can qualify as a ‘main establishment’ only if it has decision-making powers with respect to the relevant personal data processing.²⁴ Interestingly, in the French case at hand, Google had requested the *Conseil d’État* to ask the CJEU to give a preliminary ruling on Article 4(16) GDPR, but the *Conseil d’État* rejected such a request.²⁵

Finally, it is worth noting that, in a later case, the *Conseil d’État* found that the Irish DPC was not competent to act as ‘lead supervisory authority’ with respect to particular processing activities undertaken by Google. However, this was because the processing activities at hand (i.e., usage of cookies) fell under the scope of application of France’s rules implementing the EPD.²⁶ Thus, in that case, the *Conseil d’État* found that the Irish DPC was not competent on the grounds that the GDPR’s ‘one-stop-shop’ mechanism does not apply to investigations concerning possible EPD violations, and not because Google was deemed not to have a ‘main establishment’ in Ireland.

C. Analysis

1. Introduction

The definition of ‘main establishment’ in Article 4(16) GDPR resembles a house of cards. The Article is subdivided into two parts which delineate the definition slightly differently for controllers and processors. Both of these parts are in turn built around two key concepts which function as connecting factors: (i) establishment; and (ii) place of central administration. As a result, the meaning of these concepts is crucial to identify the ‘main establishment’ of a controller or processor.

2. The concept of establishment

Before trying to establish where the *main* establishment of a controller or processor is located in accordance with the criteria set out in Article 4(16) GDPR, it is first necessary to assess whether and where the relevant entity has *establishments* in the EU/EEA.²⁷ Indeed, the incipit

²¹ Ibid.

²² Ibid., para. 5.

²³ Ibid. paras. 4-5.

²⁴ EDPB 2024, para. 37.

²⁵ Ibid., para. 28.

²⁶ Conseil d’État, *Google LLC et Google Ireland Limited*.

²⁷ EDPB 2024, para. 10. Pursuant to s. 8 of Protocol 1 to the EEA Agreement, whenever the acts incorporated in the Annexes to the Agreement (like the GDPR) refer to the territory of the ‘Community’ (now, ‘Union’), such

of both point (a) and (b) of Article 4(16) makes clear that the definition of ‘main establishment’ only applies to controllers and processor ‘with establishments in more than one Member State’.²⁸

The concept of ‘establishment’ is not defined in the GDPR, but recital 22 states that ‘[e]stablishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect’. This wording essentially reproduces that of recital 19 DPD,²⁹ which led the CJEU to uphold a flexible understanding of the concept of ‘establishment’ within the meaning of the DPD.³⁰ According to the Court, the concept ‘extends to any real and effective activity — even a minimal one — exercised through stable arrangements’.³¹ However, the Court clarified that ‘both the degree of stability of the arrangements and the effective exercise of activities [in a Member State] must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned’.³² In this regard, the Court held that even the presence of a representative in a Member State could, in some circumstances ‘suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question’.³³

Against this background, the CJEU is likely to uphold a flexible understanding of the concept of ‘establishment’ in Article 4(16) GDPR and to reject a formalistic approach whereby a controller or processor is established in a Member State solely if it is formally registered or incorporated in that Member State.³⁴

3. The concept of place of central administration

Under EU law, the concept of place of central administration is intrinsically linked to that of establishment, as the latter may take the form of setting up the former in the territory of a Member State. The place of central administration is generally perceived as the place where the actual running of a company takes place (i.e. where the most important decisions are taken).³⁵ In essence, it normally corresponds to the operational headquarters or real seat of a company (*siège réel*), which does not necessarily coincide with the company’s registered office or place of incorporation (*siège statutaire*). This understanding of the term would seem broadly to pertain to Article 4(16) GDPR as well, in particular as recital 36 GDPR states that the concept

references should be understood as references to the territories of the EEA countries (i.e. the EU Member States plus Iceland, Liechtenstein and Norway).

²⁸ It should be noted that point (b) of entry 5e of Annex XI to the EEA Agreement specifies that the term ‘Member State(s)’ in the GDPR shall be understood to include, in addition to its meaning in the Regulation, the three EEA EFTA States (i.e. Iceland, Liechtenstein and Norway).

²⁹ Rec. 19 DPD stated that ‘establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements’ and that ‘the legal form of such an establishment, whether simply [a] branch or a subsidiary with a legal personality, is not the determining factor’. See also Case C-131/12, *Google Spain*, para. 48.

³⁰ See Case C-230/14, *Weltimmo*, para. 29.

³¹ *Ibid.*, para. 31. See further Case C-191/15, *Verein für Konsumenteninformation*, para. 75; Case C-210/16, *Wirtschaftsakademie*, paras. 53–55. For a critical view of the expanding scope of the concept of ‘establishment’, see Svantesson 2016.

³² See Case C-230/14, *Weltimmo*, para. 29.

³³ *Ibid.*, para. 30.

³⁴ On the concept of establishment, see further the commentaries on Arts. 3 and 4(23) in this edition.

³⁵ EDPB 2024, para. 17. See too Harvey and Schilling 2013, p. 281.

of ‘main establishment . . . should imply the effective and real exercise of management activities . . . through stable arrangements’.

The term ‘place of central administration’ is not defined in the GDPR and the Regulation makes no reference to national laws for the purpose of determining its meaning. Thus, the term should be given an autonomous EU-wide meaning.³⁶ In light of the absence of specific guidance on the meaning of the term in the GDPR’s legislative material, this meaning should be determined by recourse to sources going beyond the GDPR.³⁷ A natural source for guidance in interpreting the term is the case law on freedom of establishment, which under Article 54 TFEU applies to ‘[c]ompanies or firms formed in accordance with the law of a Member State and having their registered office, *central administration* or principal place of business within the Union’ (emphasis added).³⁸

While the CJEU has yet to define authoritatively the concept of ‘central administration’ within the meaning of the Treaties, in *Daily Mail*, Advocate General Darmon referred with approval to Everling’s interpretation of the term ‘central administration’ in Article 58 of the Treaty of Rome (i.e. the legal antecedent of Article 54 TFEU).³⁹ In particular, the Advocate General opined that:

[E]stablishment may . . . take the form of . . . the transfer of the central management and control of the company, often regarded as its real head office. That is called ‘primary establishment’. It has been said in that regard that ‘central management and control is not a legal concept but an economic one’ and that it ‘is located where the company organs take the decisions that are essential for the company’s operations’.⁴⁰

The CJEU did not directly comment on the above views of the Advocate General, but it would seem to agree with him when noting that:

[T]he transfer of the central management and control of a company to another Member State amounts to the establishment of the company in that Member State because the company is locating its centre of decision-making there, which constitutes genuine and effective economic activity.⁴¹

³⁶ The CJEU has consistently held that the need for uniform application of EU law and the principle of equality require that the terms of a provision of EU law which makes no express reference to the law of the Member States for the purpose of determining its meaning and scope be normally given an autonomous and uniform interpretation throughout the EU, having regard not only to its wording but also to the context of the provision and the objective pursued by the legislation in question: see Case C-617/15, *Hummel Holding*, para. 22 and case law cited therein. An EU-wide meaning of ‘place of central administration’ is also consistent with the aim of Art. 4(16) GDPR to create a uniform EU-wide criterion for determining which supervisory authority should be the lead supervisory authority in a particular case.

³⁷ EDPB 2024, para. 16. See too, by analogy, the way in which Advocate General Tanchev interpreted the term ‘establishment’ under the Community Trade Mark Regulation (stating that ‘[i]n the absence of guidance in the legislative material, the term “establishment” under Article 97(1) CTMR necessarily has to be determined by recourse to sources going beyond the CTMR’): see Case C-617/15, *Hummel Holding* (AG Opinion), para. 30.

³⁸ For an overview of the CJEU case law on freedom of establishment, see EC Guide 2017.

³⁹ See Everling 1964, p. 75.

⁴⁰ See Case C-81/87, *Daily Mail* (AG Opinion), para. 4. It is worth noting that the Advocate General uses the term ‘central management and control’ as equivalent to ‘central administration’. This emerges more clearly e.g. in the French and Italian versions of para. 4 of the Opinion which use the term ‘administration centrale’ and ‘amministrazione centrale’, respectively.

⁴¹ See Case C-81/87, *Daily Mail*, para. 12. Just like the Advocate General, the Court seems to treat the expressions ‘central management and control’ and ‘central administration’ as equivalent.

Similarly, in *Cartesio*, the Court appears to regard the terms ‘central administration’ and ‘real seat’ of a company as equivalent.⁴²

The case law on Article 60(1)(b) of the Brussels I Regulation (repealed) is another relevant source of inspiration for interpreting the term ‘place of central administration’ in Article 4(16) GDPR. Similarly to the GDPR, the Brussels I Regulation used the term as a connecting factor. For example, also on the basis of the Advocate General opinion cited above, the Court of Appeal held that the ‘place of central administration’ of a company within the meaning of Article 60(1)(b) of the Brussels I Regulation:

[I]s the place where the company concerned, through its relevant organs according to its own constitutional provisions, takes the decisions that are essential for that company’s operations. That is . . . the same thing as saying it is the place where the company, through its relevant organs, conducts its entrepreneurial management; for that management must involve making decisions that are essential for that company’s operations . . .⁴³

A non-formalistic understanding of the term seems to follow also from the legislative history of Article 4(16) GDPR, as several Member States unsuccessfully tried to modify the definition of ‘main establishment’ to lay down a formal connecting criterion, which referred to the place of incorporation of the relevant entity.⁴⁴ In this respect, Advocate General Bobek noted that ‘the GDPR embraces a dynamic understanding of what is considered to be the main establishment, which need not necessarily coincide with the static corporate structure of an undertaking.’⁴⁵

In view of technological developments, it can be difficult to pinpoint the ‘place of central administration’ in practice. Indeed, the directors of a company may often take part in the decision-making without being physically present in a given place — e.g. by attending a meeting via videoconference.⁴⁶

4. Main establishment of a controller

Article 4(16)(a) GDPR provides that, as rule, the ‘main establishment’ of a controller for GDPR purposes is the ‘place of its central administration’ in the EU/EEA. According to the EDPB, the implied assumption in the GDPR is that the place where decisions about the purposes and means of the processing of personal data are taken would normally coincide with the place of

⁴² See Case C-210/06, *Cartesio*, para. 105.

⁴³ Court of Appeal (England and Wales), *Young v Anglo American South Africa Limited*, para. 45. It should be noted that the Court held that the meaning of ‘central administration’ was *acte clair* and so found it unnecessary to refer the case to the CJEU under Art. 267 TFEU. The *Bundesgerichtshof* interpreted the term under the Brussels I Regulation in a similar way in its judgment XII ZB 114/06 of 27 June 2007.

⁴⁴ See e.g. Council Report 2014, p. 8, fn. 1.

⁴⁵ Case C-645/19, *Facebook Ireland and Others* (AG Opinion), para. 144.

⁴⁶ Interestingly, already in 1988, Advocate General Darmon opined that ‘[t]he concept of central management is difficult to pin down. Even where it designates the place at which the board of directors meets, it is not sufficient to provide a satisfactory connecting factor. As has been noted, owing to the progress made by means of communication, it is no longer necessary to arrange formal board meetings. The telephone, telex and telecopier enable each director to state his point of view and to take part in the decision-making without being physically present in a given place. The board meetings each director will attend via television will soon form part of a company’s everyday life’. See Case C-81/87, *Daily Mail and General Trust* (AG Opinion), para. 7. Similar remarks were also made during the legislative process that led to the adoption of the GDPR: see e.g. Council Report 2014, p. 8, fn. 1.

central administration in the EU/EEA of the controller.⁴⁷ In light of this, the ‘main establishment’ typically coincides with the controller’s European headquarters.⁴⁸

However, there may be cases where an EU/EEA establishment other than the place of central administration makes autonomous decisions concerning the purposes and means of a specific processing activity and has the power to have such decisions implemented.⁴⁹ In such case, the establishment having taken the decisions is to be considered the ‘main establishment’ of the controller. As noted by the EDPB, this means that:

[T]here can be situations where more than one lead authority can be identified, i.e. in cases where a multinational company decides to have separate decision-making centres, in different countries, for different processing activities.⁵⁰

Such other establishment may qualify as ‘main establishment’ under Article 4(16) GDPR only if it is in the EU/EEA. The general rule established by Article 4(16)(a) is that the ‘main establishment’ of a controller is ‘the place of its central administration in the Union’, and the exception to this rule is applicable only where the decisions on the purposes and means of the processing are taken in another establishment *in the Union*.

According to the EDPB, a controller’s ‘place of central administration’ in the Union can be considered as a ‘main establishment’ under Article 4(16)(a) GDPR only if it takes the decisions on the purposes and means of the processing of personal data and it has the power to have these decisions implemented.⁵¹ Consequently, it takes the view that:

[T]he one-stop-shop mechanism can only apply if there is evidence that one of the establishments in the Union of the controller takes the decisions on the purposes and means for the relevant processing operations and has the power to have these decisions implemented. Therefore, when the decisions on the purposes and means and the power to have such decisions implemented are exercised outside of the Union, there should be no main establishment under Article 4(16)(a) GDPR, and the one-stop-shop mechanism should not apply.⁵²

While the EDPB has provided several arguments in support of its reading of Article 4(16)(a) GDPR,⁵³ the view that only a ‘place of central administration’ with decision-making powers on personal data processing may qualify as a ‘main establishment’ under Article 4(16)(a)

⁴⁷ See also EDPB 2023, para. 18 (noting that ‘[t]he approach implied in the GDPR is that the central administration in the EU is the place where decisions about the purposes and means of the processing of personal data are taken and this place has the power to have such decisions implemented’). See too rec. 36 GDPR.

⁴⁸ For example, this seems to be Advocate General Bot’s understanding with regard to the data processing activities of Facebook at issue in *Wirtschaftsakademie*: ‘[under the one-stop-shop mechanism,] a controller that carries out cross-border data processing, such as Facebook, will have only one supervisory authority as interlocutor, namely the lead supervisory authority, which will be the authority for the place where the controller’s main establishment is located. Nevertheless, that scheme, and the sophisticated cooperation mechanism which it introduces, are not yet applicable . . . Facebook has chosen to set up its main establishment in the European Union in Ireland’, as the Facebook group has a European head office in Ireland, which was involved in deciding on the purposes and means of the personal data processing at issue in the case. See Case C-210/16, *Wirtschaftsakademie* (AG Opinion), paras. 51, 95 and 103.

⁴⁹ See EDPB 2023, para. 19.

⁵⁰ *Ibid.*

⁵¹ EDPB 2024, para. 37.

⁵² *Ibid.*, p. 1.

⁵³ EDPB 2024, paras. 14-27.

GDPR is not incontrovertible. This view seems to conflate the notion of ‘controller’ and that of ‘establishments of the controller’. It also downplays the fact that Article 4(16)(a) and (b) set out the ‘central administration’ criterion as the main rule for identifying the ‘main establishment’ both with respects to controllers and processors. A homogeneous interpretation of the notion of ‘central administration’ under Article 4(16)(a) and (b) would thus be at odds with the view expressed by the EDPB, as processors are never involved in making decisions on the means and purposes of the processing. Further, while recital 36 could lend some support to the position of the EDPB when it states that the main establishment ‘should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements’, this does not seem to be conclusive, as recitals are descriptive and not prescriptive in nature,⁵⁴ and the above cited passage in recital 36 does not seem to be accurately reflected in the part of Article 4(16)(a) dealing with the ‘central administration’ before the word ‘unless’. A broader reading of the ‘central administration’ criterion would also seem to be in line with the GDPR’s objective of ensuring a consistent and homogenous application of its rules across the EU/EEA (see recital 10), an objective that is better ensured when the one-stop-shop mechanism applies, which typically depends on the existence of a ‘main establishment’ in the Union. Consequently, a clarification from the CJEU would be especially warranted, in particular in view of the French case law cited above, which seems to support a different reading of Article 4(16)(a) GDPR.

The location of the ‘main establishment’ of the controller should be carefully determined by the controller itself according to objective criteria, in particular where the central administration criterion does not apply.⁵⁵ Pursuant to recital 36 GDPR, the key criterion consists in identifying the location where ‘the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements’ takes place.⁵⁶ In contrast, the place where the processing of personal data is carried out and the presence and use of certain technical means and technologies for processing personal data are not, in themselves, determining criteria.⁵⁷ In practice, according to the EDPB, the controller should consider the following non-exhaustive list of queries for determining the location of its ‘main establishment’:

1. Where are decisions about the purposes and means of the processing given final ‘sign off’?
2. Where are decisions about business activities that involve data processing made?
3. Where does the power to have decisions implemented effectively lie?
4. Where is the Director (or Directors) with overall management responsibility for the cross-border processing located?
5. Where is the controller or processor registered as a company, if in a single territory?⁵⁸

⁵⁴ On the legal nature of recitals, see Case C-673/17, Planet49 (AG Opinion), para. 71 and case law cited therein.

⁵⁵ See rec. 36 GDPR. See further EDPB 2023, para. 24 (noting that the controller’s determination of its ‘main establishment’ ‘can be challenged by the respective supervisory authority concerned afterwards’).

⁵⁶ See rec. 36. See further EDPB 2023, para. 23.

⁵⁷ See rec. 36. See too EDPB 2023, para. 23.

⁵⁸ EDPB 2023, para. 25.

In this regard, the EDPB has clarified that:

[T]he GDPR does not permit ‘forum shopping’. If a company claims to have its main establishment in one Member State, but no effective and real exercise of management activity or decision making over the processing of personal data takes place there, the relevant supervisory authorities (or ultimately EDPB) will decide which supervisory authority is the ‘lead’, using objective criteria and looking at the evidence. The process of determining where the main establishment is may require active inquiry and co-operation by the supervisory authorities. Conclusions cannot be based solely on statements by the organisation under review. The burden of proof ultimately falls on controllers and processors to demonstrate to the relevant supervisory authorities where the relevant processing decisions are taken and where there is the power to implement such decisions.⁵⁹

In essence, if a controller has a preference for a specific ‘lead supervisory authority’ (e.g. an authority with an enforcement policy that is perceived as business friendly), it may not simply claim that its ‘main establishment’ is located in the jurisdiction of that authority to ensure that the latter be entrusted with the primary responsibility for dealing with the controller’s cross-border data processing activities; the controller should instead adapt its operations so that the relevant processing decisions are taken in that jurisdiction.

The GDPR does not specifically clarify how to identify the ‘main establishment’ in case the relevant data processing activities take place under the responsibility of joint controllers. In this respect, the WP29 had initially opined that:

[T]o benefit from the one-stop-shop principle, the joint controllers should designate (among the establishments where decisions are taken) which establishment of the joint controllers will have the power to implement decisions about the processing with respect to all joint controllers. This establishment will then be considered to be the main establishment for the processing carried out in the joint controller situation. The arrangement of the joint controllers is without prejudice to the liability rules provided in the GDPR, in particular in Article 82(4).⁶⁰

However, in 2023, the EDPB changed its posture on this point,⁶¹ and made clear that joint controllers may not decide between themselves which of their establishments should be deemed the ‘main establishment’ for GDPR purposes:

[T]he decision-making power of joint controllers does not comprise the determination of the competent supervisory authority according to Articles 55 and 56 GDPR, or the ability of these supervisory authorities to exercise their tasks and powers as described in Articles 57 and 58 GDPR.

The notion of main establishment is linked by virtue of the GDPR to a single controller and cannot be extended to a joint controllership situation. This is without prejudice to

⁵⁹ EDPB 2023, para. 37. See too EDPB 2024, para. 11.

⁶⁰ WP29 2017, pp. 7–8.

⁶¹ The EDPB did not provide an extensive justification for this change. It simply stated that it ‘noticed that there was a need for further clarifications, specifically regarding the notion of main establishment in the context of joint controllership and taking into account the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR’. See EDPB 2023, para. 2.

the possibility for each joint controller to have its own main establishment. In other words, the main establishment of a controller cannot be considered as the main establishment of the joint controllers for the processing carried out under their joint control. Therefore, joint controllers cannot designate (among the establishments where decisions on the purposes and means of the processing are taken) a common main establishment for both joint controllers.⁶²

In other words, the EDPB made clear that supervisory authorities are not bound by any designation made by joint controllers.⁶³

While the original position of the WP29 had certain practical advantages for controllers, the recent clarification provided by the EDPB seems more in line with the GDPR's assumption that the 'main establishment' 'be determined according to objective criteria' and not by means of a subjective designation from the part of the (joint) controllers (see recital 36).⁶⁴ The EDPB guidance seems to imply that, in some circumstances, only one of the joint controllers may be deemed to have a 'main establishment' in the EU/EEA. This may be the case when one of the joint controllers is established in the EU/EEA, and the other is not. In such a situation, only the controller established in the EU/EEA may be considered to have a 'main establishment' in the EU/EEA if it meets the criteria of Article 4(16)(a) GDPR, as these apply 'as regards a controller with establishments *in more than one Member State*' (emphasis added). Thus, for the same processing activities, the one-stop-shop mechanism should apply with respect to only one of the joint controllers (i.e. the one with establishments in the EU/EEA), whereas the other controllers should deal with local supervisory authorities in every Member State of relevance, through their local representatives.⁶⁵ In such case, it would seem reasonable to expect that the concerned supervisory authorities cooperate to ensure that the GDPR's rules are consistently applied to the processing activities at issue.⁶⁶

5. Main establishment of a processor

In line with the main rule applicable to controllers (illustrated above), Article 4(16)(b) GDPR provides that the 'main establishment' of a processor is 'the place of its central administration in the Union'. However, if the processor has no central administration in the EU/EEA, the establishment in the EU/EEA where the main processing activities take place is to be considered the 'main establishment' of the processor.⁶⁷ The GDPR does not clarify which processing activities should be considered *main* processing activities. The indefinite scope of

⁶² Ibid., paras. 33 and 34.

⁶³ Ibid., para. 32.

⁶⁴ For a critique of the original WP29 position, see the commentary on Art. 4(16) in the first edition of this Commentary at page 234.

⁶⁵ EDPB 2023, para. 49. However, the EDPB considers that 'the creation of a main or single establishment or its relocation from a third country to the EEA (in a procedure which was initially started without cooperation) mid-procedure will allow the controller to benefit from the one-stop-shop'. See EDPB 2019, p. 8.

⁶⁶ See rec. 123 GDPR: 'The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation'.

⁶⁷ See EDPB 2023, paras. 39-40.

the latter concept makes it quite difficult to apply in practice.⁶⁸ However, one could argue — by analogy with what recital 36 states with regard to the ‘main establishment’ of a controller — that whether an activity qualifies as a ‘main processing activity’ should be determined according to objective criteria and that these may vary depending on the specific features and nature of the processing activities delegated to the processor.

The second part of Article 4(16)(b) GDPR subjects the application of the main processing activities criterion to two qualifications: (i) the processing activities need to take place ‘in the context of the activities of an establishment of the processor’; and (ii) the processor need to be ‘subject to specific obligations under [the] Regulation’. The first qualification implies that the processing of personal data does not need to be carried out ‘by’ the relevant establishment itself, rather that it is sufficient if the processing is carried out ‘in the context of the activities’ of the establishment.⁶⁹ However, if the establishment in the EU/EEA is not involved in any direct way in the processing of data, the data processing activities are normally considered to be carried out ‘in the context of the activities’ of the EU/EEA establishment only as long as there is an ‘inextricable link’ between the activities of the EU/EEA establishment and the data processing.⁷⁰

The second qualification seems merely to make clear that the GDPR applies to processors only inasmuch as this is specifically set forth in other provisions of the GDPR, and that the criteria of Article 4(16)(b) are immaterial in this regard. It worth noting that, as made clear in Recital 36: ‘In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment’.

Consequently, in such cases it is immaterial whether and where the processor has a ‘main establishment’ in the EU/EEA for GDPR purposes. In practice, this means that a processor that provide services to multiple controllers located in different Member States (e.g. a cloud provider) may have to deal with multiple supervisory authorities.⁷¹

6. Main establishment of a group of undertakings

Where the processing is carried out by a group of undertakings that has its headquarters in the EU/EEA,⁷² the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking (see recital 36 GDPR). In essence, as noted by the EDPB:

[T]he establishment of the undertaking with overall control is presumed to be the decision-making centre relating to the processing of personal data, and will therefore be considered to be the main establishment for the group, except where decisions about the purposes and means of processing are taken by another establishment. The parent,

⁶⁸ This difficulty was also noted during the legislative process where several Member States remarked that ‘in view of technological developments, it was very difficult to pinpoint the place of processing and that it was very tricky to establish a main establishment with far-reaching consequences’: see Council Report 2014, p. 8, fn. 1.

⁶⁹ See Case C-131/12, *Google Spain*, para. 52; Case C-230/14, *Weltimmo*, para. 35. See also rec. 22 GDPR.

⁷⁰ See Case C-131/12, *Google Spain*, paras. 55–57. See further WP29 2015, pp. 3–4. On the concept of ‘in the context of the activities’, see also the commentary on Art. 4(23) in this edition.

⁷¹ EDPB 2023, para. 41.

⁷² Further on the concept of ‘group of undertakings’, see the commentary on Art. 4(19) in this edition. See also rec. 37 GDPR.

or operational headquarters of the group of undertakings in the EU, is likely to be the main establishment, because that would be the place of its central administration.⁷³

The above should be considered a general rule of thumb applicable to corporate groups with centralised decision-making headquarters and a branch-type structure. However, the decision system of a corporate group could be more complex, giving independent decision-making powers relating to cross-border processing to different establishments in the EU.⁷⁴ In such case, the main establishment for the group should be determined through the above-listed criteria for identifying the main establishment of a controller or processor.⁷⁵

7. Change of main establishment

As mentioned above, the identification of the ‘main establishment’ of a controller/processor is primarily relevant to determine which national supervisory authority should be the ‘lead supervisory authority’ in a specific cross-border enforcement case. However, this competence should not be considered as definitely fixed. The controller/processor may decide to relocate or disband its main establishment. If this occurs mid-procedure before a final enforcement decision is made, this normally triggers a transfer of the lead competence to another authority (i.e. that of the new main establishment) or the termination of the applicability of the ‘one-stop-shop’ principle (if the main establishment is moved out of the EEA or disbanded).⁷⁶ Nonetheless, some supervisory authorities have argued that they remain competent to issue fining decisions with respect to GDPR violations committed before the relocation of the main establishment to another EEA country.⁷⁷

8. Conclusions

While the basic contours of the notion of ‘main establishment’ are fairly clear, applying it in practice is unlikely to be consistently plain sailing. As the EDPB aptly noted, ‘[t]here will be borderline and complex situations where it is difficult to identify the main establishment or to determine where decisions about data processing are taken’.⁷⁸ This difficulty will in turn create complications for the identification of the ‘lead supervisory authority’ and may thus hinder the smooth operation of the ‘one-stop-shop’ mechanism.

Select Bibliography

International instruments

Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS No. 108.

EEA Agreement: Agreement on the European Economic Area, OJ 1994 L 1/3.

⁷³ See EDPB 2023, para. 27.

⁷⁴ Ibid, para. 28.

⁷⁵ Ibid.

⁷⁶ See EDPB 2019.

⁷⁷ Italian DPA 2024.

⁷⁸ EDPB 2023, para. 35.

EU legislation

Brussels I Regulation: Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ 2001 L 12/1.

Community Trade Mark Regulation: CTMR: Council Regulation (EC) No. 207/2009 of 26 February 2009 on the Community trade mark, 2009 OJ L 78/1.

GDPR: 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) (Text with EEA relevance), OJ 2016 L 119/1.

Regulation 1215/2012: Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ 2012 L 351/1.

Rome I Regulation: Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), 2008 OJ L 177/6.

National legislation

German GDPR Implementation Law: Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU), BGBl 2017 Teil I Nr. 44.

Academic writings

Everling 1964: Everling, *The Right of Establishment in the Common Market* (Commerce Clearing House 1964).

Harvey and Schilling 2013: Harvey and Schilling, 'Conclusion of Contract', in Dannemann and Vogenauer (eds.), *The Common European Sales Law in Context* (OUP 2013), 248.

Svantesson 2016: Svantesson, 'Article 4(1)(a) "Establishment of the Controller" in EU Data Privacy Law—Time to Rein in this Expanding Concept?', 6(3) *International Data Privacy Law* (2016), 210.

Papers of data protection authorities

EDPB 2019: European Data Protection Board, 'Opinion 8/2019 on the competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment' (9 July 2019).

EDPB 2023: European Data Protection Board, 'Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority' (Version 2.1, 28 March 2023).

EDPB 2024: European Data Protection Board, 'Opinion 04/2024 on the notion of a main establishment of a controller in the Union under Article 4(16)(a) GDPR' (13 February 2024).

WP29 2012: Article 29 Working Party, 'Opinion 01/2012 on the Data Protection Reform Proposals' (WP 191, 23 March 2012).

WP29 2015: Article 29 Working Party, 'Update of Opinion 8/2010 on Applicable Law in Light of the CJEU Judgement in Google Spain' (WP 179 update, 16 December 2015).

WP29 2017: Article 29 Working Party, 'Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority' (WP 244 rev.01, as last revised and adopted on 5 April 2017).

CNIL 2019: Commission nationale de l'informatique et des libertés, 'Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC' (21 January 2019).

Italian DPA 2024: Garante per la protezione dei dati personali, ‘Provvedimento del 2 novembre 2024 [doc. web n. 10085455]’ (2 November 2024).

Reports and recommendations

Council Report 2014: One-stop-shop mechanism, 9327/14, 30 April 2014.

EC Guide 2017: Guide to the Case Law of The European Court Of Justice on Articles 49 et seq. TFEU—Freedom Of Establishment, Ref. Ares(2017)1839123, 6 April 2017.

EC Staff Working Paper 2012: Commission Staff Working Paper ‘Impact Assessment Accompanying the document 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) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data’, SEC(2012) 72 final, 25 January 2012.

Article 10. Processing of personal data relating to criminal convictions and offences

*TERESA QUINTEL**

Processing of personal data relating to criminal convictions and offences or related security measures based on article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by union or member state law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Relevant Recitals

(19) 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, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council. Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and 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. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

(91) This should in particular apply to large-scale processing 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

* The views and opinions expressed in this contribution are those of the author and do not necessarily reflect the official policy or position of the European Parliament. This contribution is based on the first edition of the Commentary in which Ludmila Georgieva authored the contribution on Art. 10.

example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

(97) Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. 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. 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.

CLOSELY RELATED PROVISIONS

Article 5 (Principles relating to processing of personal data); Article 6 (Lawfulness of processing) (see too recital 50); Article 9 (Processing of special categories of personal data); Article 27 (Representatives of controllers or processors not established in the Union) (see too recital 80); Article 30 (Records of processing activities) (see too recital 97); Article 35 (Data protection impact assessment) (see too recitals 75 and 91); Article 37 (Designation of the data protection officer) (see too recital 97)

RELEVANT CASE LAW

CJEU

Case C-489/10, *Lukasz Marcin Bonda*, judgment of 5 June 2012 (Grand Chamber) (ECLI:EU:C:2012:319). Case C-136/17, *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)*, judgment of 24 September 2019 (Grand Chamber) (ECLI:EU:C:2019:773).

Case C-439/19, *B v Latvijas Republikas Saeima*, judgment of 22 June 2021 (Grand Chamber) (ECLI:EU:C:2021:504).

Case C-740/22, *Endemol Shine Finland Oy*, judgment of 7 March 2024 (Sixth Chamber) (ECLI:EU:C:2024:216).

ECtHR

Leander v Sweden, Appl. No. 9248/81, judgment of 26 March 1987.
Antunes Rocha v Portugal, Appl. No. 64330/01, judgment of 31 May 2005.
M.M. v United Kingdom, Appl. No. 24029/07, judgment of 13 November 2012.
Khelili v Switzerland, Appl. No. 16188/07, judgment of 18 October 2011.
Brunet v France, Appl. No. 21010/10, judgment of 18 September 2014.

A. Rationale and policy underpinnings

The purpose of Article 10 GDPR is to ensure the responsible handling of personal data relating to criminal convictions and offences or related security measures, since they may have a significant impact on the life of the data subjects concerned. Article 10 does not prohibit the processing of such data but instead subjects them to a specific regime. Article 10 must be read in conjunction with other GDPR provisions, namely Article 5(1) (concerning the principles for processing of personal data), Article 6(1) (which governs the lawfulness of processing), Article 2(2)(d) (which exempts data processing covered by the LED from the scope of the GDPR), and with the LED. The LED covers 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.¹ Consequently, Article 10 GDPR applies to processing by private bodies and public bodies which are not competent authorities in accordance with Article 3(7) LED, or data processing which is not for the purposes listed in Article 2(2)(d) and Article 1(1) LED.

B. Legal background

1. EU legislation

In the Commission Proposal for the GDPR², the processing of criminal records was included under Article 9 (concerning the processing of special categories of personal data) and thus, prohibited unless the conditions to derogate were satisfied. Hence, the proposal structurally followed the same logic as the DPD, which devoted paragraph (5) in Article 8 ('sensitive data') to personal data related to criminal offences.

However, Article 8(5) DPD was a provision independent from other categories of sensitive data listed in Article 8(1) DPD. In fact, Article 8(5) DPD was directly leaning on Article 7 DPD, which stipulated a list of possible legal bases for processing.³ It could, therefore, be inferred that, teleologically, Article 10 GDPR follows a similar logic as a standalone provision, including a specific reference to the legal bases in Article 6(1). Nevertheless, Article 10 emphasises the separation to *other* special categories of personal data by placing the processing of criminal convictions and offences into a detached provision. This change from the original Commission proposal as outcome of the GDPR trilogue negotiations followed the advice of the WP29⁴, which argued that personal data relating to criminal convictions and offences were too different from other special categories of personal data and would deserve a standalone Article under the GDPR. The first clear separation was adopted in the General Approach in

¹ See Art. 1(1) LED.

² GDPR Proposal.

³ Dammann and Simitis 1997, p.169. See also WP29 2011, p. 6.

⁴ Ibid.

June 2015, where the Council put forward Article 9a on the processing of data relating to criminal convictions and offences.⁵

As mentioned above, another notable difference between Article 8(5) DPD and Article 10 GDPR is the scope of the provision. While the DPD covered offences, criminal convictions and security measures, the GDPR only covers criminal convictions and offences and related security measures. The GDPR narrowed the application of this provision down by covering only convictions, offences and security measures with a criminal element, while the Directive included additional types of offences (i.e. also administrative and minor offences) and unrelated security measures. In the First Reading Position of the EP,⁶ the Parliament suggested to also cover ‘administrative sanctions, judgments, criminal or suspected offences, convictions or related security measures’. However, this proposal was rejected by the Council.⁷

Besides the obvious differences stemming from the mere choice of the instrument (Directive vs. Regulation), the co-legislators seemingly attempted to introduce other novelties between the DPD and the GDPR, in order to clarify the text. Firstly, the DPD foresaw *suitable* safeguards for the processing of personal data relating to criminal convictions and offences, whereas Article 10 refers to *appropriate* safeguards. This is a horizontal change: the GDPR consistently mentions *appropriate* safeguards, while the DPD was less coherently when using *suitable* and *appropriate* safeguards. Secondly, the GDPR allows for the processing of personal data relating to criminal records when such processing is authorized by Union or Member State law, while the Directive allowed for derogations permitted under national provisions. Thirdly, the Directive referred to a *complete* register of criminal convictions whereas the GDPR speaks about *comprehensive* registers, thereby slightly expanding the scope of Article 10 in order to capture further of such registers.

2. International instruments

Article 6 of Convention 108 includes personal data relating to criminal convictions within the definition of special categories of personal data. That Article authorises the processing of special categories of data provided that domestic law provides for appropriate safeguards. As originally adopted, Convention 108 stated that ‘personal data relating to criminal convictions’ may ‘not be processed automatically unless domestic law provides appropriate safeguards’. The Explanatory Report to Convention 108 focuses on the context in which personal data may be processed rather than the actual content of the data. Hence, where processing may be particularly harmful to persons and is likely to lead to encroachments, such data should be considered to be particularly sensitive and fall under Article 6.⁸ According to the Explanatory Report, criminal convictions in the sense of Article 6 of Convention 108 should be understood as ‘convictions based on criminal law and in the framework of a criminal procedure’.

The Modernised Convention 108, albeit different in wording, follows the logic of Article 6 of Convention 108.⁹ However, it is broader than both Convention 108 and Article 10 GDPR, as it includes ‘personal data relating to offences, criminal proceedings and convictions, and related security measures’ in its specification of ‘special categories of data’ (Article 6(1)). Such data may only be processed ‘where appropriate safeguards are enshrined in law, complementing

⁵ Council Presidency Document 9398/15.

⁶ EP GDPR Legislative Resolution.

⁷ Council Presidency Document 9398/15.

⁸ Explanatory Report Convention 108 1981.

⁹ Ibid.

those of [Modernised Convention 108]’, and these safeguards ‘shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination’ (Article 6(2)).

3. National developments

By stating that data relating to criminal convictions and offences may be processed when authorised by Member State law provided there are appropriate safeguards, Article 10 GDPR leaves leeway for Member States to adopt national legislation that ensures the security, integrity and availability of personal data. Traditionally, Member States enact such legislation, for instance, to maintain public registers of criminal convictions and related information. In Germany, the *Bundeszentralregister* (‘BZR’) is a public register with information on criminal proceedings before German courts, which is maintained by the Federal Ministry of Justice and established by legislation.¹⁰

Differences in Member State law existed already with regard to the transposition of Article 8(5) of the DPD: while criminal convictions and offenses were not listed as sensitive data in Article 8 DPD, the WP29 stated that in some cases, Member States either defined them as an additional category of sensitive data or created a special legal framework including certain conditions for processing such data.¹¹

4. Case law

Both the ECtHR and the CJEU have adjudicated on the matter. The ECtHR has held that a system for the retention and disclosure of criminal record data should afford sufficient safeguards to ensure that data relating to an individual’s private life are not disclosed in violation of the right to respect for private life pursuant to Article 8 of the European Convention of Human Rights and Fundamental Freedoms (‘ECHR’). For instance, in the case of *M.M. v United Kingdom*, the ECtHR held that national arrangements for the indefinite retention and disclosure of criminal data infringed Article 8 ECHR.¹²

In *CG and Others*¹³, four applicants sought to exercise their right to de-reference certain links to third-party websites before the CJEU. The relevant websites contained sensitive data pertaining to the applicants. The Court held that, subject to derogations, the processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, and a complete register of criminal convictions may be kept only under the control of official authority.¹⁴

Interestingly, the Court stated that the content of Article 8(1) and (5) DPD was taken over in Article 9(1) and 10 GDPR, thereby linking the prohibition or restrictions with regard to special categories of personal data with Article 10 GDPR.¹⁵ Consequently, it found that an interference is, due to the sensitivity of the data, particularly serious where the processing of special categories of data mentioned in Articles 9(1) and 10 GDPR takes place.¹⁶

¹⁰ German Federal Registry Act 2017.

¹¹ WP29 2011, p. 8.

¹² ECtHR, *M.M. v UK*.

¹³ Case C-136/17, *GC and others v Commission nationale de l’informatique et des libertés (CNIL)*.

¹⁴ *Ibid.*, para. 40.

¹⁵ *Ibid.*, paras. 41, 42, 44, 67, 72, 73.

¹⁶ *Ibid.*, para. 67.

The Court held that ‘information concerning legal proceedings brought against an individual, such as information relating to the judicial investigation and the trial and, as the case may be, the ensuing conviction, is data relating to ‘offences’ and ‘criminal convictions’ within the meaning of the first subparagraph of Article 8(5) of [the DPD] and Article 10 of [the GDPR], regardless of whether or not, in the course of those legal proceedings, the offence for which the individual was prosecuted was shown to have been committed.’¹⁷ Consequently, by including those data in the list of search results, the processing of such data by the operator of a search engine would be subject to special restrictions.¹⁸

Nevertheless, the CJEU held that ‘a search engine operator does not need to automatically delete links to specific sites following an erasure request made by the data subject. Instead, in order to determine whether to remove links to pages that contain sensitive personal data, the search engine operator would have to perform a balancing test of the competing rights in presence.’¹⁹

In *B v Latvijas Republikas Saeima*, the CJEU ruled on national legislation that required the road safety authority to publish data on penalty points for traffic violations. The Court held that the processing of personal data relating to penalty points by a national administrative body handling the national register of vehicles and drivers for the purpose of road safety would fall within the material scope of the GDPR, since such authority could not be regarded a competent authority within the meaning of the LED.²⁰ At the same time, the Court found that such processing would be covered by Article 10 GDPR, thereby granting enhanced protection to the personal data processed. Taking into account the scope and application of the LED, such interpretation could lead to an unfortunate application of the Directive instead of the GDPR, as the Court qualified personal data relating to penalty points as data relating to criminal offences. While the Court probably sought to include such data within the higher protection standards under Article 10 GDPR, it simultaneously broadened the scope of the LED insofar as authorities competent under the LED could process data relating to penalty points within the scope of the Directive. With its recent *La Quadrature du Net II and Others* judgment,²¹ the Court further broadened the LED’s scope, holding that a public authority processing personal data in the course of an activity of a ‘pre-criminal nature’ directly linked to the judicial proceedings for minor offences must be classified as public authority competent under the LED.²²

This interpretation could allow additional authorities to apply the Directive to their processing activities, thereby granting them more flexibility with regard to the data minimisation and purpose limitation principles, to restrict data subject rights, or concerning international transfers.

Besides its relevant finding in *Endemol Shine Finland Oy*²³ that even information disclosed orally may constitute personal data, the CJEU held that data relating to criminal convictions contained in a court’s filing system may not be disclosed orally for the purpose of ensuring public access to documents if the person requesting the disclosure does not establish that they

¹⁷ Ibid., para. 72.

¹⁸ Ibid., para. 73.

¹⁹ Ibid., para. 80.

²⁰ Ibid., para. 71.

²¹ Case C-470/21, *La Quadrature du Net II and Others*.

²² Ibid., paras. 158 and 159.

²³ Case C-740/22, *Endemol Shine Finland Oy*.

have a specific interest in obtaining those data.²⁴ Referring to its findings in *B v Latvijas Republikas Saeima*, the Court found that the data in question were covered by Article 10 GDPR, and that that provision does not preclude personal data from being disclosed to the public where such disclosure is necessary for the performance of a task carried out in the public interest or in the exercise of official authority. However, the legislation authorising the disclosure must provide for appropriate safeguards.²⁵

5. Decisions of national data protection authorities

National DPAs have issued around 25 decisions in which they referred to Article 10 GDPR. In 2022, the national DPA in Spain imposed a €2,000,000 fine on Amazon Road Transport Spain for breaching Article 10 GDPR by requesting criminal record certificates as part of their hiring procedure.²⁶ The Italian DPA fined the Italian Bar Association €20,000 for publishing information about two complainants on their website, including details of hearings in criminal proceedings where the complainants were defendants. The DPA ruled that this processing of personal data fell under Article 10 GDPR and was conducted without a legitimate legal basis, as no law authorized the processing.²⁷ In Norway, the national DPA ordered Google to delete a search result related to a data subject's criminal past. However, it upheld Google's refusal to erase two additional search results about that individual. The DPA found these results to be still relevant after 10 years, partly because the data subject was a CSO in a company planning to go public. Thus, the DPA argued that this rendered the information a subject of public interest. The DPA's decision was confirmed on appeal.²⁸

C. Analysis

1. Introduction and scope

Article 10 addresses the protection of personal data in a particularly sensitive context, i.e. the processing of personal data relating to criminal convictions and offences or related security measures. Although personal data relating to criminal convictions and offences or related security measures are not mentioned in Article 9 GDPR (which concerns the processing of 'special categories of data'), the special sensitivity of such data and their processing is shown by the fact that they are the subject of a standalone article. The processing of such data can have severe adverse consequences for data subjects in terms of stigmatisation, the ability to find employment and discrimination in other important areas of life. Article 10 thus lays down strict conditions for the processing of such data. In particular, processing of the data covered by Article 10 must fulfil the requirements of Article 5 GDPR, be based on one of the grounds for processing under Article 6(1) GDPR,²⁹ and be conducted either under the control of official authority or authorised by Member State or EU law. Other provisions of the GDPR contain further requirements specifying the protections that must be carried out when the data described in Article 10 are processed, including maintaining records of processing activities (see Article 35), carrying out a data protection impact assessment (see Article 35(3)(b) and recital 91) or designating a data protection officer (see Article 37(1)(c) and recital 97).

²⁴ Ibid., para. 58.

²⁵ Ibid., para. 49.

²⁶ Spanish DPA 2022.

²⁷ Italian DPA 2023.

²⁸ Norwegian DPA 2022.

²⁹ Note in this regard that rec. 47 GDPR states that 'the processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned'.

Since the misuse of these types of data may entail defamatory or discriminatory consequences for data subjects, the processing of personal data under Article 10 should be regarded as similar to the processing of special categories of data provided for under Article 9 GDPR, as also clarified by the CJEU in *CG and Others*. However, both necessity and objectives to carry out the processing of personal data relating to criminal convictions and offences should be differentiated from the processing of special categories of personal data under Article 9.

The provision is directed at both public and private controllers and processors. It allows only two scenarios for the processing of personal data related to criminal convictions and offences or related security measures; under the control of official authority, or authorised by Union or Member State law.³⁰ Where the latter is the case, such law must provide for appropriate safeguards for the rights and freedoms of data subjects. This distinguishes Article 10 GDPR from Article 9, which sets out a prohibition for the processing of special categories of data but provides for derogations. Article 10 neither stipulates a prohibition nor is it a legal basis for the processing of personal data relating to criminal convictions and offences or related security measures. Furthermore, other than Article 9(2) GDPR, which requires specific grounds to derogate from the prohibition to process special categories of personal data, Article 10 GDPR mandates a legal basis ensuring appropriate safeguards. Nevertheless, the CJEU clarified that the data referred to under Article 10 GDPR are subject to specific requirements³¹ and special restrictions³² due to their particular sensitivity.

Lastly, Article 10 provides for any comprehensive register that retains personal data relating to criminal convictions to be kept under the control of official authority. Hence, the scope of Article 10 is determined by Member State law, subject to interpretation by the CJEU.³³ For instance, the CJEU has held that three criteria must be examined when determining what constitute ‘criminal offence’, namely the legal classification of the offence under national law, the intrinsic nature of the offence and the nature and the degree of severity of the penalty that the person concerned is liable to incur.³⁴

Whereas the term ‘criminal convictions’ includes only data relating to actual criminal convictions pronounced by a court or similar public authority, ‘offences’ refers to information about criminal offences even if this does not include data about an actual conviction.³⁵ Data about mere suspicions of criminal activity are not expressly covered by Article 10 or otherwise mentioned in the GDPR, and it is uncertain whether it could fall within the scope of Article 10. However, the potentially grave consequences for individuals of processing data concerning suspicions of criminal activity³⁶ suggest that the definition of ‘offences’ may be expanded by Member States to include suspicions as well. Regarding ‘security measures’, these refer to

³⁰ Kelleher and Murray 2018.

³¹ Case C-136/17, *GC and Others v Commission nationale de l’informatique et des libertés (CNIL)*, para. 44.

³² *Ibid.*, para. 73.

³³ See rec. 13 LED, stating that ‘criminal offence’ within the meaning of the LED should be an autonomous concept of Union law as interpreted by the CJEU.

³⁴ Case C-439/19, *Latvijas Republikas Saeima*, paras. 87, 88, 89. See also Case C-489/10, *Lukasz Marcin Bonda*, para. 37.

³⁵ See e.g. ECtHR, *Khelili v Switzerland*, where the Court found that the processing by the police of data that incorrectly designated the complainant as a prostitute violated her right to the respect for private life under Art. 8 ECHR; and ECtHR, *Brunet v France*, where the Court held there was a violation of Art. 8 ECHR when the complainant’s data were retained in a criminal database after the criminal proceedings against him were discontinued. See also WP29 2017, p. 7, in which the WP29 suggested that ‘offences’ under Art. 10 GDPR may include data about traffic safety and violations.

³⁶ See Dammann and Simitis 1997, p. 170.

measures addressing criminal offences without resulting in a formal conviction,³⁷ such as the revocation of a driver's license or temporary detention in a psychiatric clinic.

2. Practical relevance

In a first scenario, allowing the processing of personal data relating to criminal convictions and offences or related security measures, such processing may be carried out under the control of official authority, i.e. by duly authorised public authorities (e.g. police, criminal courts or national registers) or by private entities vested with public authority and public powers (e.g. private prisons). Wherever personal data under Article 10 are processed on behalf of such controllers (or joint controllers) by a processor that is not a public body as defined under Article 4(8) GDPR, the wording of Article 10 suggests that such controllers must be in *permanent* control of the processing, and it would not suffice if the official authority would sporadically review the processing activities (which should anyway be the case in a controller-processor relationship).

In the second scenario, where processing activities under Article 10 are authorised by Union or Member State law, such law must always be accompanied by appropriate safeguards. These safeguards could, for instance, be a developed access control and identification management system (i.e. different levels of authorisation for designated personnel in the national register of criminal convictions, limited and differentiated access for other public authorities such as police and prisons etc.), physical data security and disaster recovery measures, as well as customised and granular retention periods.

In both scenarios, the processing must be based on one of the grounds under Article 6(1) GDPR. In practice, this means that the processing activities under Article 10 have to derive their legal basis either from Union or Member State law. In the first scenario, the control of official authority should be interpreted as a stricter version of the second part of Article 6(1)(e),³⁸ while in the second scenario, the respective Union or Member State law may authorise processing for a broader variety of public and private entities, but is nevertheless limited to the two legal bases laid down in law — Article 6(1)(c) or 6(1)(e) GDPR — which must provide for appropriate safeguards for the rights and freedoms of data subjects.

Finally, comprehensive registers of criminal convictions may only be kept under the control of official authority, thus limiting the possibility to keep such registers to processing under the first scenario. Consequently, private companies may not hold any such register. The word *comprehensive* implies that the provision refers to overarching registers, e.g. national registers that either hold personal data of *all* criminal convictions, or registers that are kept only for certain parts of the population or certain types of crimes, but that are comprehensive in that aspect.³⁹

3. Article 10 GDPR in relation with other provisions in the GDPR

Article 10 GDPR must be read in conjunction with other provisions that require specific conditions whenever certain types of personal data are being processed. As mentioned above, these are, *inter alia*, Article 30(5) (records of processing activities where the processing

³⁷ Ibid.

³⁸ 'Processing 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'.

³⁹ ECtHR, *Antunes Rocha v Portugal*.

includes personal data relating to criminal convictions and offences), Article 35(3)(b) (the carrying out of a DPIA where processing of personal data relating to criminal convictions and offences is carried out) and Article 37 (the mandatory designation of a DPO).

Even controllers and processors that are enterprises or organisations employing fewer than 250 persons have to keep detailed records of the processing activities under their responsibility whenever they process personal data relating to criminal convictions and offences. Those controllers and processors are not able to enjoy the ‘lighter’ regime provided for under Article 30(5).

In accordance with Article 35(3)(b), controllers and processors processing personal data relating to criminal convictions and offences or related security measures must carry out a DPIA and seek advice of their DPO in order to determine the appropriate measures to be put in place to comply with the GDPR.⁴⁰ Such DPIA should be mandatory for personal data processed under Article 10, in particular, where such processing includes biometric data.⁴¹

Under Article 37(1)(a), a DPO should be designated where the processing is carried out by a public authority or body. For two additional reasons the designation of a DPO is particularly relevant in the context of Article 10. Firstly, private entities have to designate a DPO if their core activities consist of processing of personal data covered by Article 10. Secondly, one of the basic tasks of the DPO under Article 39 is to give advice regarding the mandatory DPIA and to monitor the latter’s performance.

As mentioned above, Article 10 GDPR may be relevant for the processing of personal data in the employment context, where, for instance, the employer requests the criminal record of a potential employee. This might be the case for professions related to tasks dealing with national security⁴², or for a public position, but also where the future employee must have a clean criminal record, e.g. when he or she is to work with children. Hence, the provision must also be read in combination with Article 88 GDPR on the processing of personal data in the employment context, as well as, with the national provisions that may be adopted under Article 88 GDPR.

4. Data processing by public authorities

Data processing by public authorities falls within the scope of the LED if they are ‘competent authorities’⁴³ and they process personal data for the purposes under Article 1(1) LED.⁴⁴ Whenever either the material or the personal scope or both are not satisfied, in most cases the GDPR applies.⁴⁵ As stated above, data processing covered by the LED is not covered by the GDPR. Conversely, this suggests that data processing not falling under the LED is covered by the GDPR, unless the processing is carried out by EU institutions, bodies, offices or agencies⁴⁶ or by national intelligence agencies for national security purposes that fall outside the scope of

⁴⁰ See, for instance, Croatian DPA.

⁴¹ Recital (91) GDPR.

⁴² ECtHR, *Leander v Sweden*.

⁴³ Art. 3(7) LED.

⁴⁴ I.e. 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. See Art. 2(2)(d) GDPR and Art. 1(1) LED.

⁴⁵ The GDPR does not apply to processing if it falls under any of the 4 categories mentioned in Art. 2(2) GDPR.

⁴⁶ In which case the EUDPR applies.

Union law.⁴⁷ The protection under the GDPR is stronger than under the LED, not only because the GDPR is a regulation while the LED is a (minimum harmonisation) directive. The transparency obligations, the possibilities to exercise one's rights and the obligations for controllers are stronger under the GDPR. Evidently, this was the will of the co-legislators, also to ensure a certain flexibility for competent authorities as referred to under Article 3(7) LED, which is necessary in the area where the Directive applies. This will was already laid down in the Lisbon Treaty.⁴⁸ Yet, it is important that those data that *should* be processed within the scope of Article 10 (and thus subject to higher protection standards under the GDPR) are not processed under the LED as this could allow more flexibility for authorities to restrict data subject rights, to apply the principles more adaptably or to have less stringent rules when it comes to international transfers. Nevertheless, Recital 19 recognises that Member States may introduce specific provisions to adapt the processing of personal data under Article 10, allowing for more precise requirements as well as potential restrictions on obligations and rights under certain conditions to safeguard key interests such as public security and crime prevention.

As mentioned above, in order to broaden the protective scope of Article 10 (also compared to its predecessor), the term 'comprehensive' record of criminal convictions under the control of official authority should be liberally interpreted to include registers that are extensive, even if they are not 100 per cent complete. The requirement of control by an official authority requires that a public authority is responsible in practice for the proper functioning of the data processing; a generic right of supervision is not sufficient.⁴⁹ An example of such control is the operation of the BZR register by the German Federal Ministry of Justice as referenced above. In that case, the Ministry of Justice is the data controller and responsible to ensure that the data in the BZR are processed in accordance with all provisions under the GDPR.

5. Data processing by private entities

Private entities and companies such as credit scoring agencies, insurance companies and businesses screening prospective employees may also seek to process data concerning criminal convictions and offences. Since processing by private entities is usually not under the control of official authority, the storing of such data by them is only permissible if EU or Member State law allows it and provides for 'appropriate safeguards for the rights and freedoms of data subjects'.⁵⁰ Recital 19 GDPR recognises that more specific national rules may allow processing by private bodies, but only under strict conditions, and, as abovementioned, that Member State legislation may also restrict 'certain rights and obligations' with regard to such processing.⁵¹

⁴⁷ See FRA 2018, p. 282.

⁴⁸ Declaration 21 attached to the Lisbon Treaty states that 'The Conference acknowledges that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields.'

⁴⁹ See Dammann and Simitis 1997, pp. 170–171.

⁵⁰ For example, as of 24 May 2018, credit agencies in Germany were no longer allowed to store data relating to criminal conviction because a specific national regulation permitting the storage had not yet been enacted: see Gola 2017, para. 9.

⁵¹ Rec. 19 GDPR states in part: 'When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and 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. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories'.

The examples given in recital 19 of ‘anti-money laundering or the activities of forensic laboratories’ indicate that such national derogations should apply only when there is a strong public interest in the processing of criminal data by private entities. The language of the recital also indicates that such derogations should be interpreted strictly in light of the EU Charter and the ECHR.

6. The European Criminal Records Information System

The European Criminal Records System (ECRIS)⁵² is a de-centralised system where all EU Member States can interconnect with each other in order to create a platform to exchange information about criminal records electronically.⁵³ The ECRIS was established in April 2012 and all EU countries are currently connected to it.⁵⁴ The system is based on a de-centralised architecture, where information is exchanged exclusively between designated Central Authorities of the Member States. Each Member State having convicted a citizen of another Member State is obliged to notify, through ECRIS, the Member State of nationality. The Member State of nationality is then obliged to store and update all information received through ECRIS, and to provide full criminal records information when requested by another Member State.⁵⁵ The ECRIS in this case serves as the platform for national authorities to ascertain whether another Member State holds criminal record information of a certain person.

The purposes of processing are, thus, the storage of criminal records information (both in ECRIS and in the Member States’ repositories), and, in a second step, the exchange of data related to convictions, and the sharing of new information regarding the convicted person (between the national authorities).

As an example, in Germany, the ECRIS Central Authority is the Federal Office of Justice (FOJ). For the above purposes related to the ECRIS, the FOJ should neither be regarded as competent authority within the meaning of Article 3(7) LED nor as processing personal data for the purposes under Article 1(1) LED, as it neither satisfies the personal nor the material scope of the Directive. Consequently, the processing of criminal records by that authority for the above purposes should fall within the scope of Article 10 GDPR, as the processing is of administrative nature and not carried out for law enforcement purposes.

In 2019, the EU co-legislators adopted the European Criminal Records System for Third Country Nationals and stateless persons (ECRIS-TCN), which complements the ECRIS with regard to individuals who are not (solely) nationals of the EU Member States. The ECRIS-TCN works according to a similar logic as the ECRIS, however, its purposes are more dispersed and could be said to include law enforcement purposes. Therefore, the ECRIS-TCN Regulation refers to both the LED and the GDPR for different processing operations.⁵⁶

In many cases, the central authority in the Member States (the controller of the ECRIS-TCN) would be part of an administrative body and thus, would generally not be permitted to process data under the LED. Although that authority receives requests for data in the context of criminal proceedings, it would not be permitted to apply the LED for processing activities, as it would

⁵² Directive 2019/884.

⁵³ A Member State is considered connected to ECRIS if it exchanges criminal records information with at least one other connected Member State.

⁵⁴ EC ECRIS.

⁵⁵ EC Report, 3.

⁵⁶ Recital 35 ECRIS-TCN Regulation.

not constitute a competent authority within the meaning of the LED. It remains to be seen how the abovementioned *Hadopi* judgment will change such approach.

During the initial search in the ECRIS-TCN, the purpose of processing would solely be the identification of the Member State holding a criminal record on a TCN, thus, not a law enforcement purpose. Such processing should fall under Article 10. Only where a competent LEA would be granted access to the ECRIS-TCN for law enforcement purposes, the processing would fall within the scope of the LED.

7. Conclusion

Article 10 brings about more clarity on the processing of personal data related to criminal convictions and offences compared to its predecessor, Article 8(5) DPD. The circumstances in which the Article allows for the processing of personal data related to criminal convictions and offences are very limited and have to be laid down in Union or Member State law. The mere fact that Article 10 is a component of the GDPR emphasises the need to clearly define the purposes of each processing operation in question. The LED does not cover personal data solely because they are ‘criminal data’, but only if they are processed within the limited realm of law enforcement tasks and by competent authorities. The case of the ECRIS-TCN Regulation demonstrates the difficulties that may arise regarding the applicability of either Article 10 GDPR or the LED. In order to achieve a proper delineation between the two instruments and to refer to the correct instrument in subsequent legislative acts, the co-legislators will have to ensure that those acts clearly distinguish between the purposes of processing, the context in which personal data falling within the remit of Article 10 are being processed, and the controllers processing the data.

Select Bibliography

International instruments

Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS No. 108.

EU legislation

Directive 2019/884: Directive (EU) 2019/884 of the European Parliament and of the Council of 17 April 2019 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, OJ L 151.

ECRIS-TCN Regulation: Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, OJ L 135.

EUDPR: 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 (Text with EEA relevance), OJ 2018 L 295/39.

GDPR: 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) (Text with EEA relevance), OJ 2016 L 119/1.

LED: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119/89.

National legislation

German Federal Registry Act 2017: Bundeszentralregistergesetz in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, 1985 I S. 195), das zuletzt durch Artikel 1 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2732) geändert worden ist.

Academic writings

Dammann and Simitis 1997: Dammann and Simitis, *EU-Datenschutzrichtlinie* (Nomos Verlagsgesellschaft 1997).

Gola 2017: Gola, ‘Art. 10’ in Gola (ed.), *Datenschutz-Grundverordnung VO (EU) 2016/679—Kommentar* (C. H. Beck 2017), 308.

Kelleher and Murray 2018: Kelleher and Murray, *EU Data Protection Law* (Bloomsbury Publishing Plc 2018).

Papers of data protection authorities

EDPS 2023: European Data Protection Supervisor, ‘Opinion 22/2023 on the Proposal for a Directive on deposit protection, cross-border cooperation and transparency’ (12 June 2023).

WP29 2011: Article 29 Working Party, ‘Advice Paper on Special Categories of Data’ (4 April 2011).

WP29 2017: Article 29 Working Party, ‘Opinion 03/2017 on Processing Personal Data in the Context of Cooperative Intelligent Transport Systems (C-ITS)’ (WP 252, 4 October 2017).

Italian DPA 2023: Garante per la protezione dei dati personali, ‘Order of 31 August 2023’ (9938413).

Norwegian DPA 2022: Datatilsynets, ‘Orders of 17 August 2021 and 15 February 2022’ (20/02059-9).

Spanish DPA 2022: Agencia Española de Protección de Datos, ‘Order of 11 February 2022’ (Nº: PS/00267/2020).

Reports and recommendations

Council Presidency Document 9398/15: 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), 9398/15, 1 June 2015.

Council of the European Union, ‘Working Document on general technical questions and issues of data protection regarding the Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011’, 10682/2017, 3 October 2017.

Council of the European Union, ‘General Approach on the Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011’, 15101/17, 30 November 2017.

EC Report: Report from the Commission to the European Parliament and the Council concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States, COM(2020) 778 final, 21 December 2020.

European Parliament, ‘Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011’, PE 612.310 v02-00, 1 February 2018.

EP GDPR Legislative Resolution: European Parliament legislative resolution of 12 March 2014 on the 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)0011 — C7-0025/2012 — 2012/0011(COD)), P7_TA(2014)0212, 12 March 2014.

Explanatory Report Convention 108 1981: Council of Europe, ‘Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data’ (28 January 1981).

FRA 2018: European Union Agency for Fundamental Rights, European Court of Human Rights, Council of Europe, and European Data Protection Supervisor (eds.), *Handbook on European Data Protection Law* (Publications Office of the European Union, 2018).

Others

Croatian DPA: Republic of Croatia Personal Data Protection Agency, ‘List of the types of processing for which a DPIA shall be required pursuant to article 35.4 GPDR, from 13 December 2018 (13 December 2018), available at https://www.edpb.europa.eu/sites/default/files/decisions/list_of_the_types_of_processing_for_dpia_croatia_35_4.pdf.

EC ECRIS: European Commission, ‘European Criminal Records Information System (ECRIS)’ (accessed on 24 February 2025), available at https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/tools-judicial-cooperation/european-criminal-records-information-system-ecris_en.

Article 17. Right to erasure ('right to be forgotten')

*HERKE KRANENBORG**

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
 - (a) the personal data are no longer necessary in relation to the purpose for which they were collected or otherwise processed;
 - (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
 - (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
 - (d) the personal data have been unlawfully processed;
 - (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
 - (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of the available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
 - (a) for exercising the right of freedom of expression and information;
 - (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
 - (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
 - (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
 - (e) for the establishment, exercise or defence of legal claims.

Relevant Recitals

(65) A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union

* The views expressed are solely those of the author and do not necessarily reflect those of the European Commission.

or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

(66) To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

CLOSELY RELATED PROVISIONS

Article 5 (Principles relating to processing of personal data); Article 19 (Notification obligation regarding rectification or erasure of personal data or restriction of processing); Article 21 (Right to object) (see also recitals 69–70)

RELEVANT CASE LAW

CJEU

Case C-617/10, *Åklagaren v Hans Åkerberg Fransson*, judgment of 26 February 2013 (Grand Chamber) (ECLI:EU:C:2013:105).

Case C-399/11, *Stefano Melloni v Ministerio Fiscal*, judgment of 26 February 2013 (Grand Chamber) (ECLI:EU:C:2013:107).

Case C-131/12, *Google Spain SL v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, judgment of 13 May 2014 (Grand Chamber) (ECLI:EU:C:2014:317).

Opinion of Advocate General Jääskinen in Case C-131/12, *Google Spain SL v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, delivered on 25 June 2013 (ECLI:EU:C:2013:424).

Case C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*, judgment of 9 March 2017 (ECLI:EU:C:2017:197).

Opinion of Advocate General Szpunar in Case C-136/17, *G.C. and Others v Commission nationale de l'informatique et des libertés (CNIL)*, delivered on 10 January 2019 (ECLI:EU:C:2019:14).

Opinion of Advocate General Szpunar in Case C-507/17, *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)*, delivered on 10 January 2019 (ECLI:EU:C:2019:15).

Case C-136/17, *G.C. and Others v Commission nationale de l'informatique et des libertés (CNIL)*, judgment of 24 September 2019 (Grand Chamber) (ECLI:EU:C:2019:773).

Case C-507/17, *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)*, judgment of 24 September 2019 (Grand Chamber) (ECLI:EU:C:2019:772).

Opinion of Advocate General Pitruzzella in Case C-460/20, *T.U. and R.E. v Google LLC*, delivered on 7 April 2022 (ECLI:EU:2022:271).

Case C-129/21, *Proximus v Gegevensbeschermingsautoriteit*, judgment of 27 October 2022 (ECLI:EU:C:2022:833).

Case C-460/20, *T.U. and R.E. v Google LLC*, judgment of 8 December 2022 (Grand Chamber) (ECLI:EU:C:2022:962).

Case C-60/22, *U.Z. v Federal Republic of Germany*, judgment of 4 May 2023 (ECLI:EU:C:2023:373).

Joined Cases C-26/22 and C-64/22, *U.F. and A.B. v Land Hessen ("Schufa II")*, judgment of 7 December 2023 (ECLI:EU:C:2023:958).

Case C-46/23, *Újpesti Polgármesteri Hivatal*, judgment of 14 March 2024 (ECLI:EU:C:2024:239).

Case C-200/23, *Agentsia po vpsivaniyata*, judgment of 4 October 2024 (ECLI:EU:C:2024:827).

ECtHR

M.B. v France, Appl. No. 22115/06, judgment of 10 May 2010.

Axel Springer AG v Germany (Grand Chamber), Appl. No. 39954/08, judgment of 7 February 2012.

Węgrzynowski and Smolczewski v Poland, Appl. No. 33846/07, judgment of 16 July 2013.

Delfi AS v Estonia, Appl. No. 64569/09, judgment of 16 June 2015.

M.L. and W.W. v Germany, Appl. Nos. 60798/10 and 65599/10, judgment of 28 June 2018.

Gaughran v United Kingdom, Appl. No. 45245/15, judgement of 13 June 2020.

Biancardi v Italy, Appl. No. 77419/16, judgment of 25 November 2021.

Hurbain v Belgium (Grand Chamber), Appl. No. 57292/16, judgment of 4 July 2023.

France

French Council of State (*Conseil d'État*), *Google LLC/CNIL*, 27 March 2020, N° 399922.

Germany

German Federal Constitutional Court (*Bundesverfassungsgericht*), decisions 1 BvR 16/13 and 1 BvR 276/17 of 6 November 2019 ('Right to be forgotten I' and 'Right to be forgotten II').

A. Rationale and policy underpinnings

The right to be forgotten in Article 17 has been perceived as one of the novelties of the GDPR and as an illustration of the modernisation of the European data protection rules. A closer look shows, however, that the right to be forgotten is in fact more of a detailed elaboration of the already existing right of erasure. This is also illustrated by the actual title of Article 17 'the right to erasure' which is followed by a reference to the right to be forgotten between brackets.

That being said, compared to the previous rules, the right to erasure or to be forgotten is given more prominence in the GDPR. This recognises its increased importance in today's society, in which personal data are generated, made public and shared on a massive scale, as an instrument for the data subject to retain a certain control over personal data.

If personal data are being processed in breach of the provisions of the GDPR, the data subject can require the controller to erase the data. The controller must also take reasonable steps to inform other controllers with whom the data were shared. As follows from Article 17, the right, as well as the obligation on the controller, is not absolute. There are several reasons which justify a limitation of the right of erasure, such as the reconciliation with the freedom of expression or the establishment, exercise or defence of legal claims.

B. Legal background

1. EU legislation

The right to erasure was also contained in the DPD in the provision on the right of access, Article 12.¹ The provision granted data subjects the right to obtain from the controller, as appropriate, the rectification, erasure and blocking of data the processing of which did not comply with the provisions of the DPD (see Article 12(b) thereof). Data subjects also had the right to obtain from the controller notification to third parties to whom the data were disclosed of any rectification erasure or blocking carried out in compliance with Article 12(b), unless it proved impossible or involved disproportionate effort (see Article 12(c) of the DPD). Thus Article 12 of the DPD already contained the basic components of what is referred to in Article 17 GDPR as the right to be forgotten.

2. International instruments

The right to erasure can be found in Article 8(c) of Convention 108, which refers to the right ‘to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention’. In Convention 108+, this has been revised in Article 9(e) to refer to the right ‘to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Convention’. Neither version of the Convention contains an additional reference to the right to be forgotten, as in Article 17 GDPR.

3. National developments

The right to erasure does not apply if, amongst other things, the processing is necessary for exercising the right to freedom of expression and information. The scope of this exception may depend on Member State law. This follows from Article 85 GDPR which requires Member States by law to reconcile the right to the protection of personal data pursuant to the GDPR with the right to freedom of expression and information, including processing for journalistic purposes and the purpose of academic, artistic and literary expression.

4. Case law

The right to erasure is also referred to as the “right to be forgotten” because of the rulings of the CJEU in which it looked at requests from data subjects for delisting search results when searching on those data subjects’ names with use of the internet search engine operated by Google.² The first of these rulings was the seminal *Google Spain* case in which a Spanish citizen asked Google Spain to remove a link to two publications in a Spanish newspaper from the list of results when searching on his name. The publications, upon order of a Spanish Ministry, announced a real-estate auction connected with proceedings for the recovery of social security debts, mentioning the name of the person. This judgment, which was based on the provisions of the DPD, as well as the subsequent rulings of the CJEU concerning Google will be further discussed below. The right to erasure was also considered by the CJEU in the *Manni* case, which concluded that this right did not require a Member State to remove limited but

¹ See on the roots of the right to be forgotten Bartolini and Siry 2016.

² See for an overview of case law of the ECtHR and the CJEU on the right to be forgotten: ECtHR and FRA Joint Factsheet 2024.

necessary personal data from a public companies register, or at least to end the general public nature of such information after a certain period of time. In the accompanying press release, the CJEU presented the decision as considering that ‘there is no right to be forgotten in respect of personal data in the companies register’.³ Nevertheless, the CJEU did not exclude the possibility that in specific situations, overriding and legitimate reasons relating to the specific case of the person concerned could justify, exceptionally, that access to personal data concerning him should be limited.⁴

The case law of the ECtHR on the right to erasure focusses mainly on the deletion of data collected and stored by national authorities in databases which are held for criminal law enforcement purposes.⁵ These matters fall outside the scope of the GDPR. However, in more recent years, the ECtHR has been confronted with cases concerning the continued availability of personal data on the internet, in particular in the online archives of newspapers. In the *Hurbain v Belgium* ruling of 2023 the Grand Chamber of the ECtHR clarified the scope of the ‘right to be forgotten online’. In this case a newspaper publisher was ordered to anonymise the online archived version of an article lawfully published twenty years earlier, on the basis of the ‘right to be forgotten’ of the subject of the article, a driver who caused a fatal accident. This ruling is further discussed in section C-6 below. In these cases, the ECtHR had to reconcile the right to freedom of expression in Article 10 ECHR, in particular the freedom of the press, with the right to privacy in Article 8 ECHR.

C. Analysis

1. Introduction

The right to erasure and the ‘right to be forgotten’ in the online environment have triggered a significant debate. This is illustrated by the great number of academic, journalistic and (other) internet publications. A big driver behind the production of all these publications was the CJEU ruling in *Google Spain*. The case constituted a perfect example of the challenges surrounding the right to erasure in modern society. It revealed the tension between freedom of expression and the personal rights of individuals and the particular impact of the internet on the dissemination of information, and it raised questions about the role and responsibilities of a search engine like Google.

Strictly speaking, the *Google Spain* ruling concerned the possibility of finding a document published on the internet by searching the internet for the individual’s name. The outcome was that the links to the website on which the document was to be found should be removed from the list of results produced by the search engine within the EU⁶ when searching on the applicant’s name. However, the document itself — an article published in a Spanish newspaper — remained publicly accessible, and could still be referenced in search results outside the EU. In consequence, the information about the person is not really ‘forgotten’, but rather removed from the ‘active memory’ of the internet. Still, the impossibility of finding the document by searching against the data subject’s name clearly reduces the ‘public impact’ of the publication on the data subject.

³ EC Press Release Manni, p. 1.

⁴ Case C-398/15, *Manni*, para. 60.

⁵ See for example ECtHR, *M.B. v France* and ECtHR, *Gaughran v United Kingdom*.

⁶ See the discussion of territorial scope below.

2. Grounds for exercising the right

The right to erasure can be invoked against any controller who processes personal data, if one of the grounds listed in Article 17(1) GDPR applies.⁷ The different grounds partly overlap. Three of them assume the lack of a basis for processing, such as if the personal data are no longer necessary for the purpose for which they were collected or otherwise processed (subparagraph (a)), consent is withdrawn (subparagraph (b)) or the personal data are unlawfully processed (subparagraph (d)).

Article 17(1)(d) can be seen as a general clause, which is confirmed by recital 65 in which it is stated that the right to erasure can be invoked by a data subject, where the processing of his or her personal data does not otherwise comply with this Regulation. In *U.Z.*, the CJEU considered that not every breach of a provision of the GDPR leads to unlawful processing within the meaning of Article 17(1)(d).⁸ In order to be lawful, processing must comply with the provisions of Chapter II GDPR. In contrast, non-compliance with the requirements of Chapter IV does not necessarily lead to unlawful processing. For example, the CJEU considered that the absence of an arrangement determining joint responsibility (Article 26 GDPR) or of a record of processing activities (Article 30) is not sufficient in itself to establish the unlawfulness of the data processing.⁹ The obligations in these provisions are not among the grounds for lawfulness of processing which are set out in Article 6(1), and, unlike Articles 7 to 11, Articles 26 and 30 are not intended to clarify the scope of the requirements set out in Article 5(1)(a) and Article 6(1).¹⁰

The three other grounds in paragraph 1 do not as such assume unlawful data processing. Article 17(1)(c) is based on an invocation of the right to object in Article 21 when processing is based on Article 6(1)(e) or (f) GDPR.¹¹ Under Article 21(1), the burden of proof following an objection has been reversed: the data controller, rather than the data subject, has to demonstrate compelling legitimate grounds for processing the data. If the controller fails to do so, the data have to be erased.¹² In case of direct marketing, the controller has to erase the data upon a simple objection of the data subject (see Article 21(2) and (3) GDPR). Article 17(1)(e) requires erasure if this is mandated under Union or Member State law. The last ground on which the right to erasure can be based is laid down in Article 17(1)(f) and concerns the situation in which the personal data have been collected in relation to the offer of information society services directly to a child, as referred to in Article 8(1). It follows from recital 65 that this ground intends to protect children who, at the time the data were collected, might not be fully aware of the risks involved by the processing. The data subject can exercise the right, notwithstanding the fact that he or she is no longer a child.¹³

⁷ Art. 17(1) does not only contain a right to erasure, it also contains a standalone obligation borne by the controller to erase data, in particular if the processing is unlawful. In that respect, a supervisory authority can order a controller to erase the data, regardless of whether the data subject has invoked its right under Art. 17(1). See Case C-46/23, *Újpesti Polgármesteri Hivatal*, paras. 37 and 42. See on the grounds for requesting delisting also: EDPB 2020.

⁸ Case C-60/22, *U.Z.*, paras. 55-58. The considerations of the CJEU apply also to Art. 18(1)(b) GDPR. See further the commentary on Art. 18 in this edition.

⁹ *Ibid.*, para. 65-66.

¹⁰ *Ibid.*, para. 59-60.

¹¹ See the commentary on Art. 21 in this edition.

¹² See also Joined Cases C-26/22 and C-64/22, *Schufa II*, para. 110-112.

¹³ See further the commentary on Art. 8 in this edition.

3. Obligation of paragraph 2

Once the right to erasure is successfully invoked, and none of the situations in the third paragraph apply (see below), the controller, if it has made the personal data public, is obliged to inform controllers who are processing those personal data that the data subject has requested the erasure by such controllers of any links to, or copies or replications of, those personal data (see Article 17(2)). According to recital 66 this obligation was introduced in order to strengthen the right to be forgotten in the online environment. According to the CJEU, it specifically applies to information made available on the internet by search engine providers that process data published online.¹⁴

The controller has to take reasonable steps, taking into account available technology and the means available to it, including technical measures, to inform other controllers which are processing the personal data of the data subject's erasure request. This obligation on the controller has been slightly weakened compared to the initial proposal of the Commission. In the proposed Article 17, the controller had to take *all* reasonable steps and was 'considered responsible' for the publication of the personal data if it 'authorised' a third party to do so.¹⁵

Although there might be a certain overlap, the obligation in Article 17(2) must be distinguished from the obligation in Article 19 GDPR, which requires the controller to notify recipients to whom the personal data have been disclosed about an erasure.¹⁶ Article 17(2) applies to the situation in which personal data has been *publicly* disclosed by the controller, and entails an obligation of conduct ("take reasonable steps") to inform other controllers about the data subject's request for erasure of links to, or copies or replications of the personal data. Article 19, on the other hand, generally concerns the disclosure of personal data to recipients and entails an obligation of result (unless it is impossible or involves disproportionate effort), regardless of whether the data subject has requested the controller to do so.¹⁷

In *Proximus*, the CJEU concluded that a provider of public directories of subscribers of telephone services is required to ensure that reasonable steps are taken to inform search engine providers of the request addressed to it by the subscriber of a telephone service for erasure of their personal data.¹⁸ The CJEU added that in order to assess the reasonableness of the steps taken by the provider of such directories, the available technology and the cost of implementation must be taken into account, which is a task that falls primarily upon the authority competent for such matters, subject to judicial review.¹⁹

The EDPB gave the example of video recordings which are stored. Data subjects may request them to be erased under Article 17 GDPR.²⁰ If the video footage has been made public (e.g., by broadcasting or streaming online), the controller must take reasonable steps to inform other controllers of the request pursuant to Article 17 (2) GDPR.²¹ The personal data can be considered erased if the picture is blurred with no retroactive ability to recover the personal data the picture previously contained.²²

¹⁴ Case C-129/21, *Proximus*, para. 93.

¹⁵ See Art. 17(2) GDPR Proposal.

¹⁶ See also the commentary on Art. 19 in this edition.

¹⁷ *Ibid.*

¹⁸ Case C-129/21, *Proximus*, para. 96.

¹⁹ *Ibid.*

²⁰ EDPB 2019, p. 20.

²¹ *Ibid.*

²² *Ibid.*

4. Exemptions

The right to erasure does not apply in the situations indicated in the third paragraph of Article 17. These situations apply regardless of the ground in the first paragraph on which the right to erasure is based. The exemption when processing is necessary for exercising the right of freedom of expression and information (subparagraph (a)) will be analysed below when the rulings of the CJEU concerning Google and the case law of the ECtHR are discussed. Other exemptions are the necessity for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (subparagraph (b)). These situations refer to the grounds for processing contained in Article 6(1)(c) and (e) GDPR.

In some circumstances, the exemption in Article 17(3)(b) can have a specific relationship with the first paragraph of Article 17. On the basis of Article 17(1)(d), data subjects can invoke the right to erasure if they consider that the processing of their personal data is unlawful. The alleged unlawfulness may concern reliance on the grounds for processing in Article 6(1)(c) and/or (e), as the data subject could claim that the law at issue does not meet the requirements of Article 6(3). In such circumstances, Article 17(1)(d) and the exemption in Article 17(3)(b) require the same assessment, namely whether the entity concerned can validly rely on Article 6(1)(c) and/or (e). If the conclusion is negative, the exemption of Article 17(3)(b) does not apply, and the data subject's right to erasure must be executed on the basis of Article 17(1)(d) (if no other exemptions apply). If the conclusion is positive, the exemption of Article 17(3)(b) applies, and the data subject cannot rely on Article 17(1)(d). However, if in relation to Article 6(1)(e), the conclusion is that the law at issue meets the requirements of Article 6(3), the data subject could still invoke the right to object under Article 21(1), which could bring the situation back to Article 17(1)(c). The CJEU has dealt with the relationship between, on the one hand, Article 17(1)(c) and (d) and, on the other hand, Article 17(3)(b) in the *Agentsia po vprisvaniyata* ruling.²³

Article 17(3)(b) was also at issue in the *Manni* ruling. In this case, the question was whether the right to erasure could be invoked with regard to limited personal data (relating to the identity and the respective functions of persons in relation to a specific company) contained in a public companies register. The CJEU first assessed whether the continued inclusion of the personal data in the public register was justified and necessary for the objective pursued (to protect the interests of third parties in relation to joint stock companies and limited liability companies).²⁴ After reaching a positive conclusion on this, the CJEU considered that the Member States could not guarantee that the natural persons whose personal data is contained in the public register have the right to obtain, as a matter of principle, after a certain period of time, erasure of the personal data concerning them.²⁵ According to the CJEU this did not result in a disproportionate interference with the rights of the individuals as laid down in Articles 7 and 8 CFR. However, the CJEU did not exclude the possibility that in specific situations, overriding and legitimate reasons relating to the specific case of the person concerned could justify, exceptionally, that access to personal data concerning him should be limited.²⁶ In such circumstances the right to erasure would not result in the actual deletion of the personal data, but would rather remove the data from the public domain.

²³ Case C-200/23, *Agentsia po vprisvaniyata*, paras. 103-105, 109-111 and 118-119.

²⁴ Case C-398/15, *Manni*, para. 52.

²⁵ Case C-398/15, *Manni*, para. 56.

²⁶ *Ibid.*, paras. 57–61. See also C-200/23, *Agentsia po vprisvaniyata*, paras. 124-125.

Another exemption to the right to erasure is when the processing is necessary for certain grounds provided for in Article 9, the provision on the processing of special categories of personal data (Article 17(3)(c)).²⁷ The same holds true for processing necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR (Article 17(3)(d)).²⁸ This particular exception can be invoked only insofar as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing. The final situation in which the right does not apply is in case of processing necessary for the establishment, exercise or defence of legal claims (Article 17(3)(e)).

5. Google and the right to be forgotten

The CJEU has considered four cases concerning Google and the right to be forgotten. The first three rulings were decided on the basis of the DPD, although in the second and third cases the CJEU did refer to the GDPR. In the fourth ruling the questions referred to the CJEU by the national court explicitly concerned the interpretation of Article 17(3)(a) GDPR.

5.1 The Google Spain ruling

The first case was the already mentioned *Google Spain* case, in which the CJEU considered that Google needed to consider the delisting of certain search results if the person requests it to do so. In its analysis, the CJEU took into account the framework of “responsibilities, powers and capabilities” of the search engine operator as the controller of the processing carried out when running the search engine.²⁹ From this, it followed that the operator only needed to perform the balancing exercise *ex post*, that is, in a specific case, when a data subject requests the dereferencing of links containing such information.³⁰

Following a request for delisting, Google had to balance the different interests at issue.³¹ The CJEU did not expend many words on freedom of expression as such. It identified three interests at stake in the balance: the economic interest of Google, the legitimate interests of internet users potentially interested in having access to the information, and the interests of the data subject.³² The interest of the newspaper itself in the wider accessibility of its website was not taken into account.³³ The role of Google as an instrument of freedom of expression in that respect was also not directly acknowledged by the CJEU.³⁴ When giving guidance as to what elements should be taken into account when striking the balance between the different interests mentioned, the CJEU referred to elements which seem to be directly taken from the case law of the ECtHR on Articles 8 and 10 ECHR. The point of departure, according to the CJEU, is that the rights of the data subject ‘as a rule’ override the other interests. However, in some

²⁷ See the commentary on Art. 9 in this edition.

²⁸ See the commentary on Art. 89 in this edition.

²⁹ Ibid., paras. 38 and 83.

³⁰ Ibid., paras. 47-48.

³¹ Case C-131/12, *Google Spain*, para. 99.

³² Case C-131/12, *Google Spain*, para. 81.

³³ Advocate General Szpunar in his opinion in Case C-136/17, *G.C. and Others* advised the CJEU to require the inclusion of the freedom of expression of the website holder as guaranteed by Art. 11 of the Charter of Fundamental rights of the European Union (‘CFR’) in the balancing exercise by Google when assessing a request for delisting, see Case C-136/17, *G.C. and Others* (AG Opinion), para. 89.

³⁴ The Court does refer to the ‘important role’ played by search engines, but only to underline that its activities constitute a more significant interference with the data subject’s fundamental right to privacy than the publication on the website, see Case C-131/12, *Google Spain*, paras. 80 and 87. See for criticism on this point Hijmans 2014.

circumstances the rights of the general public might prevail. According to the CJEU, this depends on the nature of the information in question, its sensitivity for the data subject's private life, and the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.³⁵

The CJEU's ruling in *Google Spain* has been criticised for not giving sufficient weight to freedom of expression.³⁶ In the subsequent cases, discussed below, the CJEU seemed to respond to the criticism by referring explicitly to Article 11 of the Charter, however, only in relation to the right of freedom of information of internet users potentially interested in accessing that webpage by means of a search on the data subject's name.³⁷ The CJEU did not go as far as also including the interest of the website holder under Article 11 of the Charter in the balancing exercise to be made.³⁸

Another point of criticism concerned the burden on the search engine operator as data controller to decide on whether or not to delist, a position that Advocate General Jääskinen had warned against in his opinion. He stated that internet search-engine service providers should not be saddled with such an obligation. According to the Advocate General this would lead to an interference with the freedom of expression of the publisher of the webpage, who would not enjoy adequate legal protection in such a situation, and would amount to the censorship of published content by a private party.³⁹ This position has been echoed in the academic literature.⁴⁰

5.2 The GC and Others ruling: what if special categories of personal data are concerned?

In the second case, *GC and Others*, the main question was whether, in case a request for delisting concerns a special category of personal data, the prohibition to process such data, as laid down in Article 8 DPD and Article 9 GDPR, applies also to a search engine as operated by Google.⁴¹ The links for which dereferencing was requested included a satirical photomontage relating to a female politician that was placed on YouTube pseudonymously, press articles mentioning one of the applicants in his capacity as public relations officer of the Church of Scientology, the judicial investigation of a male politician, and the sentencing of an individual for sexual assaults on minors.

The CJEU considered that the prohibition of Article 8 DPD and, now, Article 9 GDPR applies to Google when it processes special categories of personal data, subject to the exceptions provided for in those provisions. However, in view of the 'responsibilities, powers and capabilities' of the search engine operator as the controller of the processing carried out when

³⁵ Case C-131/12, *Google Spain*, paras. 81 and 97. See on this also Kranenborg 2015, pp. 77–79.

³⁶ See Frantziou 2014, Kuner 2015, Kulk and Zuiderveen Borgesius 2015. On tension between the right to be forgotten and freedom of expression in general, see Fazlioglu 2013.

³⁷ See, e.g., Case C-136/17, *GC and Others*, paras. 66, 68, 69 and 75.

³⁸ In two parallel cases on the right to be forgotten in relation to a website holder and Google as the operator of a search engine, the *Bundesverfassungsgericht* did take into account the interest of the website holder when assessing whether the search engine operator performed a proper balancing exercise. See *Bundesverfassungsgericht*, decisions 1 BvR 16/13 and 1 BvR 276/17 of 6 November 2019. See about these decisions: Wendel 2020.

³⁹ Case C-131/12, *Google Spain* (AG Opinion), para. 134. See Allen 2015 for an elaborate comparison of the opinion of the AG and the CJEU ruling.

⁴⁰ See e.g. Spiecker 2015, p. 1053.

⁴¹ Case C-136/17, *GC and Others*.

running the search engine, the Court ruled that the prohibition is only triggered when a data subject requests the dereferencing of links containing such information.⁴²

The CJEU looked into two of the exceptions to the prohibition, namely processing based on consent and processing relating to personal data that are manifestly made public by the data subject.⁴³ The CJEU concluded that, in relation to the right to be forgotten, processing based on consent will not be of much practical value, in particular since Article 7(3) of the GDPR confirms that the data subject is entitled to withdraw consent at any time.⁴⁴ Moreover, such withdrawal is explicitly mentioned as a ground for invoking the right in Article 17 GDPR.⁴⁵ In contrast, the CJEU accepted the lawfulness of the processing of special categories of data which are manifestly made public, without, however, developing this point much further.⁴⁶ The CJEU underlined that, *in any event*, the person concerned can object to the reference in the search results, and that following a request for dereferencing, the search engine operator must assess whether maintaining the link would be necessary for exercising the right of freedom of information of the internet user potentially interested in accessing that website by means of a search on the name of that person concerned.⁴⁷ The basis for this assessment for the CJEU is to be found in Article 8(4) DPD and Article 9(2)(g) GDPR, in which Member State or Union law, for reasons of substantial public interest may add exceptions to the general prohibition to process special categories of personal data.⁴⁸ The Court made it clear that this consideration must be seen against the background of Article 17(3)(a) GDPR.⁴⁹

GC and Others also dealt with personal data relating to offences and criminal convictions within the meaning of Article 8(5) DPD and Article 10 GDPR. Although these are treated differently to the ‘other’ special categories of personal data in both instruments, the CJEU basically applied the same logic, namely that a request for dereferencing ultimately implies a balancing exercise against the right of freedom of information of the user of the search engine.⁵⁰ When providing further substantive guidance, the CJEU referred to the *M.L. and W.W. v Germany* ruling of the ECtHR, which will be discussed in Section C–6 below.

With regard to personal data relating to offences and criminal convictions, the CJEU considered that the search engine operator must assess whether, in the light of all the circumstances of the case, displaying the information is still relevant.⁵¹ As factors to consider the CJEU mentions the nature and seriousness of the offence in question, the progress and the outcome of the proceedings, the time elapsed, the part played by the data subject in public life and his or her past conduct, the public’s interest at the time of the request, the content and form of the publication and the consequences of publication for the data subject. The CJEU added that if the operator concludes the link should be maintained, it is required, at the latest on the occasion of the request for dereferencing, to adjust the list of results in such a way that the overall picture it gives the internet user reflects the current legal position, which means in particular that links to webpages containing that information must appear first on the list.⁵²

⁴² Ibid., paras. 47–48.

⁴³ Ibid., para. 61. These exceptions can be found in Art. 8(1)(a) and (e) DPD and Art. 9(2)(a) and (e) GDPR.

⁴⁴ Ibid., para. 62.

⁴⁵ See Art. 17(1)(b) GDPR.

⁴⁶ Case C-136/17, *GC and Others*, paras. 63–64.

⁴⁷ Ibid., para. 66.

⁴⁸ Ibid.

⁴⁹ Ibid., paras. 59–60.

⁵⁰ Ibid., para. 75.

⁵¹ Ibid., para. 77.

⁵² Ibid.

5.3 The Google v CNIL ruling: what is the territorial effect of the right to be forgotten?

The third ruling, *Google v CNIL*, concerned the geographical effects of a successful request for delisting.⁵³ In order to help Google and other search engines to organise compliance with the *Google Spain* ruling, the WP29 issued guidelines on the implementation of the ruling.⁵⁴ When it turned out that Google was delisting persons from search results only when the search was performed from Google websites with domains within the EU, the former WP29 sent a letter to Google, warning that the decision of delisting must guarantee the effective and complete protection of data protection rights and that EU law cannot be circumvented.⁵⁵ After Google was fined by the French CNIL because of the refusal to apply the delisting to all of its search engine's domain name extensions, the question reached the CJEU in the subsequent court proceedings. Advocate General Szpunar in his opinion in the case advised the CJEU not to give the right global scope, but to require that it be limited to searches executed within the EU, thus preventing persons located within EU territory from seeing the delisted results when using the Google search engine.⁵⁶

The CJEU considered that the EU legislator could have the competence to lay down the obligation for a search engine provider to carry out a dereferencing on all the versions of the search engine, giving it worldwide effect.⁵⁷ However, the CJEU concluded that although the legislator, in Article 17(3)(a) GDPR, struck a balance between the right to data protection and the freedom of information of internet users within the Union, it had not done so for dereferencing outside the Union.⁵⁸ It followed that, as Union law stood, there was no obligation to carry out a dereferencing on all the versions of the search engine.⁵⁹ The position taken by the CJEU seems to be motivated by the considerations that 'numerous third States do not recognise the right to de-referencing or have a different approach' and that the balance between the rights to privacy and data protection and the freedom of information of internet users 'is likely to vary significantly around the world'.⁶⁰

As to the territorial effect of a successful request for delisting within the Union, the CJEU considered that the dereferencing should not be limited to the version of the search engine corresponding to the Member State of residence of the person concerned.⁶¹ Since the data protection rules are laid down in a regulation, which is directly applicable in all the Member States, which should ensure a consistent and high level of protection throughout the Union and remove the obstacles to flows of personal data within the Union, dereferencing is, in principle, supposed to be carried out in respect of all the Member States for searches conducted from the territory of the Union on the basis of the data subject's name.⁶² According to the CJEU it is for the search engine operator to take, if necessary, sufficiently effective measures to ensure the effective protection of the data subject's fundamental rights. Those measures must themselves meet all the legal requirements and have the effect of preventing or, at the very least, seriously

⁵³ Case C-507/17, *Google v CNIL*.

⁵⁴ See WP29 2014. It should be noted that the WP29 had taken the view in an earlier opinion that a search engine provider was generally not to be held primarily responsible under European data protection law, see WP29 2008, p. 23.

⁵⁵ See WP29 Letter Google Spain. See also Kranenborg 2015, pp. 76–77.

⁵⁶ Case C-507/17, *Google Inc.* (AG Opinion), paras. 63 and 74–75. See on the matter also Van Calster 2018.

⁵⁷ *Ibid.*, para. 58.

⁵⁸ *Ibid.*, para. 61.

⁵⁹ *Ibid.*, paras. 64–65.

⁶⁰ *Ibid.*, paras. 59–60.

⁶¹ *Ibid.*, para. 66.

⁶² *Ibid.*, paras. 66 and 69.

discouraging internet users in the Member States from gaining access to the links in question using a search conducted on the basis of that data subject's name.⁶³

The CJEU considered that even within the Union the result of weighing up the interests of privacy and data protection and the freedom of information might vary and will not necessarily be the same for all the Member States, especially since under Article 85 GDPR it is for the Member States to provide for exemptions and derogations necessary to reconcile the rules on protection of personal data with, inter alia, the freedom of information.⁶⁴ In that respect, the CJEU pointed to the consistency mechanism in the GDPR which provides national supervisory authorities with the instruments and mechanisms necessary to reconcile a data subject's rights to privacy and the protection of personal data with the interest of the public throughout the Member States in accessing the information in question. Accordingly, they may adopt, where appropriate, a dereferencing decision which covers all searches conducted from the territory of the Union on the basis of that data subject's name.⁶⁵

Google v CNIL ends with a quite puzzling consideration. The CJEU emphasised that even while Union law does not require worldwide dereferencing, it does not prohibit it either. A supervisory or judicial authority of a Member State remains competent to weigh up, in the light of national standards of protection of fundamental rights, a data subject's right to privacy and the protection of personal data concerning her or him, on the one hand, and the right to freedom of information, on the other, and, after weighing those rights against each other, to order, where appropriate, the operator of that search engine to carry out a de-referencing concerning all versions of that search engine.⁶⁶ On this point, the CJEU omitted a phrase that occurs in the case law to which it refers (*Åkerberg Fransson* and *Melloni*), namely that Member States may do so 'provided that the level of protection provided for by the Charter, as interpreted by the Court, and the primacy, unity and effectiveness of European Union law are not thereby compromised'.⁶⁷ It is precisely this condition which seems to stand in the way of Member States granting worldwide effect to a dereferencing. In the end, the French referring court decided that there was no statutory authorisation under French law for extraterritorial jurisdiction.⁶⁸

5.4 The *T.U. and R.E. v Google LLC* ruling: what role for the accuracy of the information concerned?

In the fourth case, *T.U. and R.E. v Google LLC*, the question was asked what role the alleged inaccuracy of the information concerned plays when Google is confronted with a request for delisting.⁶⁹ The case concerned persons about whom articles were written and published on the internet which allegedly contained inaccurate claims and defamatory opinions. It raised a tricky question for the CJEU, as requiring Google to take into account the accuracy of the information at issue could imply that Google would have to establish what information on the internet is accurate or not and thus become the arbiter of truth on the internet. The referring court asked the

⁶³ Ibid., para. 70.

⁶⁴ Ibid., para. 67.

⁶⁵ Ibid., paras. 68-69.

⁶⁶ Ibid., para. 72.

⁶⁷ Case C-617/10, *Åkerberg Fransson*, para. 29; Case C-399/11, *Melloni*, para. 60.

⁶⁸ Conseil d'État, *Google LLC/CNIL*.

⁶⁹ The analysis will be limited to the first question referred to in the case. A second question raised was essentially whether the approach set out in *Google Spain* also applied to searches on images, which results in a list of thumbnails. The CJEU basically confirmed this, thereby emphasising the particularly significant interference with the rights to privacy and data protection brought about by displaying pictures of a person. See Case C-460/20, *T.U. and R.E. v Google LLC*, para. 94, and the full analysis in paras. 88-108.

CJEU whether delisting in such a case should be subject to the condition that the question of accuracy has been resolved, at least provisionally, in a court action brought by the person against the publisher of the information where there is a reasonable possibility of obtaining such judicial protection.

The CJEU considered that the accuracy of the information concerned is a relevant factor when balancing the different interests under Article 17(3)(a).⁷⁰ In line with the opinion of Advocate General Pitruzzella, the CJEU considered that in cases in which the freedom of expression in principle overrides the rights to private life and data protection, in particular where the data subject plays a role in public life, that situation is reversed where, at the very least, a part — which is not minor in relation to the content as a whole — of the information proves to be inaccurate.⁷¹

The CJEU then navigated quite subtly between the data subject and Google as regards the burden of proof. On the one hand, the person requesting delisting must establish “the manifest inaccuracy” of the information.⁷² However, in order to avoid imposing an excessive burden on that person, he or she has to provide “only evidence that [...] can reasonably be required of him or her”.⁷³ In that regard, the person cannot be required, in principle, to produce a judicial decision against the publisher of the information, even in the form of a decision in interim proceedings.⁷⁴ On the other hand, the operator of the search engine cannot be required ‘to play an active role’ in trying to find facts which are not substantiated by the request for de-referencing.⁷⁵ The operator does not need to investigate the facts and, to that end, organise an adversarial debate with the content provider, as Advocate General Pitruzzella had suggested.⁷⁶ According to the CJEU this would go beyond what can reasonably be expected from the operator in the light of its ‘responsibilities, powers and capabilities’.⁷⁷ It follows that if the data subject submits ‘relevant and sufficient evidence capable of substantiating his or her request and of establishing the manifest inaccuracy of the information’ which is not minor in relation to the content as a whole, the operator of the search engine must delist the search result.⁷⁸ In case national proceedings are instigated by the data subject against the publisher of the information concerning the alleged inaccuracy, the operator has to add a warning to the relevant search result if the proceedings have been brought to its attention.⁷⁹

6. What about the publisher?

Whether the right to be forgotten could also relate to the removal of the information from the internet as such, was not addressed in the *Google Spain* case. The CJEU did not deal with this question as it made a clear distinction between the responsibilities of Google as the search engine on the one hand, and the responsibilities of the publisher of a website on the other hand. Since the questions put before it only related to Google, the CJEU did not go into the responsibility of the publisher of the website. The Court only stated that the search engine

⁷⁰ Case C-460/20, *T.U. and R.E. v Google LLC*, para. 64.

⁷¹ *Ibid.*, para. 65, with reference to Case C-460/20, *T.U. and R.E. v Google LLC* (AG Opinion), para. 30.

⁷² Case C-460/20, *T.U. and R.E. v Google LLC*, para. 68.

⁷³ *Ibid.*

⁷⁴ *Ibid.*

⁷⁵ *Ibid.*, para. 70.

⁷⁶ *Ibid.*, para. 71. See Case C-460/20, *T.U. and R.E. v Google LLC* (AG Opinion), para. 45.

⁷⁷ *Ibid.*

⁷⁸ *Ibid.*, para. 72.

⁷⁹ *Ibid.*, para. 76.

might be obliged to remove the results from the list, even when the publication of the information to which a result refers in itself was lawful.⁸⁰

The ECtHR steps into this lacuna. The ECtHR has not dealt yet with a case concerning the delisting of results by the operator of an internet search engine. However, in *Hurbain v Belgium*, the Grand Chamber of the ECtHR gave an extensive explanation of the state of play concerning the right to be forgotten in the online environment and the distinct roles the initial publishers and the operators of a search engine have. In that case, a newspaper publisher was ordered to anonymise the online archived version of an article lawfully published twenty years earlier, on grounds of the ‘right to be forgotten’ of the driver who caused a fatal accident who was named in the article. With reference to *M.L. and W.W. v Germany*, the ECtHR underlined that because of the amplifying effect on the dissemination of information and the nature of the activity underlying the publication of information on the person concerned, the obligations of search engines towards the individual who is the subject of the information may differ from those of the entity which originally published the information.⁸¹ The forms of processing performed by the search engine and the original publisher are different, each with its own grounds of legitimacy and with different impacts on the individual’s rights and interests.⁸² In consequence, data subjects are not obliged to contact the original website, either beforehand or simultaneously, in order to exercise their rights *vis-à-vis* search engines.⁸³

Until the Grand Chamber ruling in *Hurbain v Belgium*, the ECtHR, when assessing measures requiring online newspapers to delete, anonymise or de-index publications contained in their online archives, assessed the matter against the well-established criteria in the ECtHR’s case law on conflicts between freedom of press and the right to privacy.⁸⁴ These are: the contribution to a debate of public interest; whether the person concerned is well known; the subject of the news report; the prior conduct of the person concerned; the way in which the information was obtained and its veracity; the content, form and consequences of the publication; and the severity of the measure imposed on the applicant.⁸⁵ The only exception was the case *Biancardi v Italy* which concerned a request for the owner of an online newspaper to de-index an article and in which a chamber of the ECtHR limited the criteria needed to be taken into consideration in weighing up the rights at stake to the length of time for which the article was kept online, the sensitiveness of the data and the gravity of the sanction imposed.⁸⁶

In *Hurbain v Belgium*, the ECtHR did not take over the approach in *Biancardi v Italy* but adjusted the well-established criteria. According to the ECtHR the balancing to be carried out in the context of a request to alter journalistic content that is archived online should take into account the following criteria⁸⁷:

⁸⁰ Case C-131/12, *Google Spain*, para. 88. See on the liability of a news website for comments on its articles posted by third persons, ECtHR, *Delfi AS v Estonia*, para. 140 and following.

⁸¹ ECtHR, *Hurbain v Belgium*, para. 207, with reference to ECtHR, *M.L. and W.W. v Germany*, para. 71 and further.

⁸² ECtHR, *Hurbain v Belgium*, para. 208.

⁸³ *Ibid.*

⁸⁴ See e.g. ECtHR, *Axel Springer AG v Germany*, paras. 89-95. On the right to be forgotten and the ECHR, see also Wechsler 2015.

⁸⁵ ECtHR, *Hurbain v Belgium*, para. 203.

⁸⁶ *Ibid.*, para. 204, with reference to ECtHR, *Biancardi v Italy*, paras. 57-71. See for a critical analysis of this ruling, as well as the chamber ruling in *Hurbain v Belgium*, Docksey 2022.

⁸⁷ ECtHR, *Hurbain v Belgium*, para. 205.

- (i) the nature of the archived information;
- (ii) the time that has elapsed since the events and since the initial and online publication;
- (iii) the contemporary interest of the information;
- (iv) whether the person claiming entitlement to be forgotten is well known and his or her conduct since the events;
- (v) the negative repercussions of the continued availability of the information online;
- (vi) the degree of accessibility of the information in the digital archives; and
- (vii) the impact of the measure on freedom of expression and more specifically on freedom of the press.

The ECtHR concluded in *Hurbain v Belgium* that the anonymisation of the contested article did not impose an excessive and impracticable burden on the publisher, while constituting the most effective means of protecting the person's privacy.⁸⁸ In its assessment the ECtHR underlined the serious harm suffered by the person concerned as a result of the continued online availability of the article, which, according to the ECtHR, was apt to create a 'virtual criminal record', especially in view of the length of time that had elapsed since the original publication of the article.⁸⁹

Throughout its case law the ECtHR underlines the importance of the principle of preservation of the integrity of press archives.⁹⁰ The alteration and, *a fortiori*, the removal of archived content must be limited to what is strictly necessary, in order to prevent any chilling effect such measures may have on the performance by the press of its task of imparting information and maintaining archives.⁹¹

In *Węgrzynowski and Smolczewski v Poland* the question was whether a press article concerning the applicant had to be removed from the archives of a newspaper's website, after it was established in Court that the publication of the article as such had infringed the rights of the applicant. The ECtHR considered that an adequate remedy to protect the rights of the applicant would be to add a comment to the article on the website informing the public of the outcome of the court proceedings. Deleting the whole article from the archive could amount to rewriting history and would be contrary to the legitimate interest of the public in access to the public internet archives of the press which is protected under Article 10 ECHR.⁹²

Select Bibliography

International instruments

Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS No. 108.

Convention 108+: Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data 2018, CM/Inf(2018)15-final.

⁸⁸ ECtHR, *Hurbain v Belgium*, para. 255.

⁸⁹ Ibid.

⁹⁰ Ibid., para. 211.

⁹¹ Ibid.

⁹² See ECtHR, *Węgrzynowski and Smolczewski v Poland*, paras. 65 and 66.

EU legislation

GDPR: 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) (Text with EEA relevance), OJ 2016 L 119/1.

GDPR Proposal: 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, 25 January 2012.

Academic writings

Ausloos, *The Right to Erasure: Safeguard for Informational Self-Determination in a Digital Society?* (Dissertation KU Leuven, 2018).

Ausloos, *The right to erasure in EU data protection law* (OUP 2020).

Allen 2015: Allen, 'Remembering and Forgetting: Protecting Privacy Rights in the Digital Age', 1(3) *European Data Protection Law Review 'EDPL'* (2015), 164.

Bartolini and Siry 2016: Bartolini and Siry, 'The Right to Be Forgotten in the Light of the Consent of the Data Subject', 32(2) *Computer Law & Security Review* (2016), 218.

Erdos, *European Data Protection Regulation, Journalism, and Traditional Publishers: Balancing on a Tightrope?* (OUP 2019).

Fabbrini and Celeste, 'The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders', *German Law Journal* (2020), 55.

Fazlioglu 2013, Fazlioglu, 'Forget Me Not: The Clash of the Right to Be Forgotten and Freedom of Expression on the Internet', 3 *International Data Privacy Law* (2013), 149.

Frantziou 2014: Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Española de Protección de Datos', 14(4) *Human Rights Law Review* (2014), 761.

Hijmans 2014: Hijmans, 'Right to Have Links Removed: Evidence of Effective Data Protection', 21(3) *Maastricht Journal of European and Comparative Law* (2014), 555.

Kuczerawy and Ausloos, 'From Notice-and-Takedown to Notice-and-Delist: Implementing Google Spain', 14(2) *Colorado Technology Law Journal* (2016), 219.

Kranenborg 2015: Kranenborg, 'Google and the Right to be Forgotten', 1(1) *EDPL* (2015), 70.

Kulk and Zuiderveen Borgesius 2015: Kulk and Zuiderveen Borgesius, "'Freedom of Expression" and "Right to Be Forgotten" Cases in the Netherlands after Google Spain', 1(2) *EDPL* (2015), 113.

Kuner 2015: Kuner, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges', in Hess and Mariottini (eds.), *Protecting Privacy in Private International and Procedural Law and by Data Protection* (Ashgate/Nomos 2015), 19.

Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press 2011).

Spiecker 2015: Spiecker, 'A New Framework for Information Markets: Google Spain', 52(4) *Common Market Law Review* (2015), 1033.

Van Calster 2018: Van Calster, 'Not Just One, but Many 'Rights to Be Forgotten'', 7(2) *Internet Policy Review* (2018), 1.

Wechsler 2015: Wechsler, 'The Right to Remember: The European Convention on Human Rights and the Right to be Forgotten', 49(1) *Columbia Journal of Law and Social Problems* (2015), 135.

Wendel 2020: Wendel, 'The two-faced guardian — or how one half of the German Federal Constitutional Court became a European fundamental rights court', *Common Market Law Review* (2020), 1383.

Papers of data protection authorities

EDPB 2019: European Data Protection Board, 'Guidelines 3/2019 on the processing of personal data through video devices (version for public consultation)' (10 July 2019).

EDPB 2020: European Data Protection Board, 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engine cases under the GDPR (part 1) (version 2.0)' (7 July 2020).

WP29 2008: Article 29 Working Party, 'Opinion 1/2008 on Data Protection Issues Related to Search Engines' (WP148, 4 April 2008).

WP29 2014: Article 29 Working Party, 'Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González C-131/12"' (WP 225, 26 November 2014).

WP29 Letter Google Spain: Article 29 Working Party, 'Letter of 6 January 2015 to Google on the Right to Be Delisted' (6 January 2015).

Others

Docksey 2022: Docksey, 'Journalism on trial and the right to be forgotten', available at: [Journalism on trial and the right to be forgotten – Verfassungsblog](#).

ECtHR and FRA Joint Factsheet 2024: European Court of Human Rights and the European Union Agency for Fundamental Rights, 'Joint Factsheet on the Right to be forgotten — ECtHR and CJEU Case-Law' (31 August 2024), available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2024-factsheet-right-to-be-forgotten_en.pdf.

EC Press Release Manni: European Commission, 'The Court Considers that There Is No Right to Be Forgotten in Respect of Personal Data in the Companies Register' (9 March 2017), available at <https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-03/cp170027en.pdf>.

Article 32. Security of processing

LEE A. BYGRAVE*

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
 - (a) the pseudonymisation and encryption of personal data;
 - (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.
4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Relevant Recital

(83) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

CLOSELY RELATED PROVISIONS

Recitals 75–79; recital 88; Article 4(12) (Definition of a personal data breach); Article 5(1)(f) (Principle of integrity and confidentiality); Article 25 (Data protection by design and by default) (see too recital 78); Article 28(1) (Choice of processor providing sufficient guarantees) (see too recital 81); Article 28(3)(c) (Processor must be contractually bound to implement security measures); Article 33 (Personal data breach notification requirement)

* This contribution is based on the first edition of the Commentary in which Cédric Burton authored the contribution on Art. 32.

to the supervisory authority) (see too recitals 85 and 87); Article 34 (Communication of a personal data breach to the data subject) (see too recital 86); Article 70(1)(g) and (h) (Tasks of the Board)

RELEVANT CASE LAW

CJEU

Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, judgment of 8 April 2014 (Grand Chamber) (ECLI:EU:C:2014:238).

Opinion 1/15, Opinion of 26 July 2017 (Grand Chamber) (ECLI:EU:C:2017:592).

Case C-340/21, *VB v Natsionalna agentsia za prihodite*, judgment of 14 December 2023 (ECLI:EU:C:2023:986).

Case C-768/21, *TR v Land Hessen*, judgment of 26 September 2024 (ECLI:EU:C:2024:785).

ECtHR

Z v Finland, Appl. No. 22009/93, judgment of 25 February 1997.

I v Finland, Appl. No. 20511/03, judgment of 17 July 2008.

S and Marper v United Kingdom, Appl. Nos. 30562/04 and 30566/04, judgment of 4 December 2008.

PN v Germany, Appl. No. 74440/17, judgment of 11 June 2020.

Podchasov v Russia, Appl. No. 33696/19, judgment of 13 February 2024.

Germany

German Federal Constitutional Court (Second Senate) (*Bundesverfassungsgericht*), decision of 8 August 1978 ('Kalkar I'), BVerfGE 49, 89.

German Federal Constitutional Court (First Senate) (*Bundesverfassungsgericht*), judgment 1 BvR 370/07 and 595/07 of 27 February 2008 (ECLI:DE:BVerfG:2008:rs20080227.1bvr037007).

A. Rationale and policy underpinnings

Data security has become increasingly important in today's data-driven society, just as data breaches have become increasingly common.¹ It could be said that the issue is not *if* a data controller or processor will suffer a data breach, but *when*. Data breaches can obviously pose substantial data protection risks. To prevent such breaches, the GDPR imposes a general security obligation on both controllers and processors. Recital 83 summarises the essence of this general obligation as follows: 'In order to maintain security ... the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks'.

Data security also underlies many of the obligations to which controllers and processors are subject under the GDPR. For example, compliance with the 'integrity and confidentiality' principle enshrined in Article 5(1)(f) or the accountability principle directed at controllers under Article 5(2) cannot be ensured unless adequate security is provided for the data being processed. This is also recognised by recital 83, which explains that security measures need to be implemented not just 'in order to maintain security', but also 'to prevent processing in infringement of this Regulation'.

It is important to keep in mind that data security on its own may serve a broader range of concerns than data protection. It can be aimed at safeguarding the interests of users of all kinds of data (not just personal data), and these interests may extend well beyond data subjects' privacy-related interests. The same can be said with the overlapping policy domains of network and information security, information systems security and cybersecurity. In these domains,

¹ See e.g. ENISA Report, p. 1, stating that '[c]yber attacks are increasing in complexity and severity, with reported incidents growing at 41% p.a.'.

the security measures are chiefly aimed at ensuring that data are processed according to the expectations of those who are authorised to steer or use a given information system or network. The primary sub-goals for these measures are maintenance of the confidentiality, integrity and availability of data in an information system or network as well as appropriate protection of the system or network itself.² In this context, ‘confidentiality’ indicates that the data and system or network are protected from unauthorised disclosure, ‘integrity’ describes their protection from unauthorised modification, and ‘availability’ denotes that they are accessible and usable on demand by authorised actors, systems or programmes.³ These sub-goals — along with others, such as authenticity (i.e. the property that data are what they are supposed to represent or convey)⁴ — are also operationalised in the GDPR’s provisions. Yet, although measures to achieve them may promote data protection, they may also come into conflict with it. Thus, the interaction between data security, data protection and privacy safeguards is complex and not always harmonious.⁵

There is an obvious connection between Article 32, Article 33 (notification of a personal data breach to the supervisory authority) and Article 34 (communication of a personal data breach to the data subject) GDPR. As a practical matter, whether Article 32 has been complied with often becomes clear in the context of a potential data breach,⁶ although, as pointed out in Section B4 below, the occurrence of a breach does not in itself necessarily imply lack of compliance. The definition of ‘personal data breach’ is contained in Article 4(12).⁷

Other provisions in the GDPR, particularly Article 5(1)(f) (principle of integrity and confidentiality), are also closely tied with Article 32. The latter is a direct manifestation and extension of Article 5(1)(f). This is not to say that the two provisions are fully commensurate. While Article 32 overlaps with and embodies Article 5(1)(f), only controllers (not controllers and processors) have primary responsibility for complying with Article 5 principles (Article 5(2) GDPR). Moreover, Article 5(1)(f) lays down a general principle for data processing whereas Article 32 concerns the measures that must be implemented to ensure observance of that principle.

Article 25 (data protection by design and by default), Article 24 (responsibility of the controller) and Article 5(2) (principle of accountability) are other GDPR provisions with a close connection to Article 32. An important constituent of this connection is the provisions’ common emphasis on the need to implement technical and organisational measures to achieve desired outcomes in the light of perceived risk. This emphasis reflects a regulatory approach oriented towards risk management and design of information systems architecture — as elaborated in section C2 below.

² See rec. 49 GDPR (defining ‘network and information security’ as ‘the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems ...’). The phrasing of rec. 49 parallels the definition of ‘network and information security’ in Art. 4(2) of the NIS Directive and Art. 6(2) of the NIS2 Directive.

³ See e.g. Hermann and Pridöhl 2020; ISO/IEC 2018, clauses 3.10, 3.36, 3.7.

⁴ ISO/IEC 2018, clause 3.6.

⁵ Further on this interaction within the EU legal framework, see Porcedda 2023, especially ch. 1.

⁶ See WP29 2018, p. 10, stating that ‘the failure to notify a breach could reveal either an absence of existing security measures or an inadequacy of the existing security measures’. On 25 May 2018, the EDPB adopted Endorsement 1/2018, in which it endorsed the WP29 paper on data breaches (inter alia): see EDPB 2018.

⁷ See the commentary on Art. 4(12) in this edition.

B. Legal background

1. EU legislation

Article 17 DPD was the equivalent to Article 32 GDPR. It specified that ‘the controller must implement appropriate technical and organizational [*sic*] measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized [*sic*] disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing’. Recital 46 DPD also articulated the need to maintain an appropriate level of security by controllers in order to prevent any unauthorised processing and listed the criteria to be taken into account when identifying the most appropriate security measures. The major difference between the security provisions of the DPD and those of the GDPR is that, unlike the DPD, the GDPR also brings processors directly under the scope of data security obligations. Article 17 DPD applied directly to controllers, and applied to processors only indirectly by providing in Article 17(3) that the use of processors had to be governed by a contract between the controller and the processor, and this contract required the security obligations of Article 17(1) to apply to the processor as well.⁸ Another difference between Article 17 DPD and Article 32 GDPR is in terms of detail: the latter’s specification of appropriate measures is considerably more elaborate than the former’s.

With respect to electronic communications, Article 4(1) EPD imposes security requirements similar to the DPD, but it is limited to providers of publicly available electronic communications services. Directive 2018/1972 establishing the European Electronic Communications Code (EECC) also mandates that providers take ‘appropriate and proportionate technical and organisational measures’ to manage the risks posed to the security of networks and service (Article 40 EECC).

In the context of law enforcement cooperation, Article 32 has an equivalent in Article 29 LED. However, the LED specifically refers to the risks related to the processing of special categories of data and identifies specific measures to be implemented in case of automated processing (e.g. equipment access control, data media control, storage control, user control etc.).⁹

In the context of processing of personal data by EU institutions, Article 32 has an equivalent in Article 33 EUIDPR. The two provisions are identical in all major respects.

Data security requirements are also set out in a multitude of other EU legislative instruments, reflecting the rapid growth — particularly over the last ten years — in EU cybersecurity law as a field in its own right.¹⁰ Many of these requirements extend to non-personal data, thus augmenting the GDPR’s requirements. Examples include the Payment Services Directive (Directive (EU) 2015/2366 (PSD2)),¹¹ the Digital Operational Resilience Act (Regulation (EU) 2022/2554 (DORA)) covering financial services,¹² the two Network and Information Security Directives (Directive (EU) 2016/1148 (NISD); repealed) and Directive (EU) 2022/2555 (NIS2D)), the Cybersecurity Act (Regulation (EU) 2019/881), the Medical Devices Regulation

⁸ However, some national laws implementing the DPD already imposed security obligations directly on processors even before the GDPR. See e.g. Art. 16(4) Belgian Data Protection Law 1992.

⁹ For further analysis of Art. 29 LED, see Markou 2023.

¹⁰ For an overview, see Bygrave 2025.

¹¹ See in particular Arts. 95–98 PSD2 Directive.

¹² See in particular Art. 9 DORA.

(Regulation (EU) 2017/745 (MDR)),¹³ the Artificial Intelligence Act (Regulation (EU) 2024/1689 (AIA))¹⁴ and, most recently, the Cyber Resilience Act (Regulation (EU) 2024/2847 (CRA)).

Of these legislative instruments, the Cybersecurity Act is particularly noteworthy. It strengthens the role of ENISA (the European Union Agency for Cybersecurity) and provides the legal footing for an EU-wide cybersecurity certification framework for digital products, services and processes — a framework intended to complement the GDPR’s certification scheme established under Article 42 GDPR.

Another particularly noteworthy instrument is the NIS2 Directive due to its horizontal scope of application. It has greater coverage than the first NIS Directive, adopting an ‘all hazards’ approach to security and eliminating the distinction applied by its predecessor between security requirements for essential services on the one hand and security requirements for digital service providers on the other. It also lays down more stringent security requirements to address the security of supply chains and supplier relationships. It goes further than its predecessor in attempting to harmonise Member States’ sanctions regimes. Fines cannot be imposed under the Directive where one has been imposed under the GDPR for the same infringement.¹⁵

The latest major addition to the EU’s legislative framework for data security is the Cyber Resilience Act. The legislation is essentially aimed at enhancing the security of the myriad connected digital devices that constitute the Internet of Things (IoT) but is pitched in broader terms. It applies to ‘products with digital elements’ — i.e. ‘a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately’ (Article 3(1) CRA).¹⁶ The basic rule is that such products shall only be placed on the EU market when they conform to ‘essential cybersecurity requirements’ as listed in Annex I of the Act (Article 6 CRA). For most products, conformity assessment is done by the manufacturers themselves. Certain products, however, are subject to a stricter assessment regime. These are products that are critical for the cybersecurity of other products or that have functions carrying a ‘significant risk’ of adversely disrupting or damaging a ‘large number of other products or ... the health, security or safety of its users through direct manipulation, such as a central system function, including network management, configuration control, virtualisation or processing of personal data’ (Article 7(2) CRA; see also recital 43 CRA). Some such products — labelled ‘important’ and listed in Annex III (e.g. identity management systems and firewalls) — must undergo conformity assessment by third parties (Articles 7(1), 32(2) and 32(3) CRA); other such products — labelled ‘critical’ and listed in Annex IV (e.g. smartcards and smart meter gateways) — must undergo certification in accordance with an approved European certification scheme (Article 8 CRA).

Importantly for present purposes, the CRA flags several synergies with the GDPR, the most obvious being that its ‘essential cybersecurity requirements’ will ‘contribute to enhancing the

¹³ See in particular Art. 10(1) Medical Devices Regulation and para. 17(2) of Annex I to the regulation.

¹⁴ See in particular Art. 15 AIA.

¹⁵ Art. 35(2) NIS2 Directive.

¹⁶ Non-commercial, open-source software products not placed on the EU market are exempted from CRA coverage (rec. 18 CRA). The same applies for products that are already covered by security requirements under other legislation — the case, for instance, with medical devices covered by the MDR (rec. 25 CRA). Most of the Act’s provisions are not legally applicable until 11 December 2027 (Art. 71(2) CRA).

protection of personal data and privacy of individuals’ (recital 32 CRA).¹⁷ It also notes organisational-institutional synergies, first regarding cybersecurity standardisation and certification: in these areas, the CRA encourages cooperation between the Commission, European standardisation bodies, ENISA, the EDPB and national DPAs (recital 32 CRA). The second set of synergies concern monitoring and enforcement: in these areas, the CRA requires national market surveillance authorities to cooperate with DPAs and empowers the latter ‘to request and access any documentation created or maintained under this Regulation when access to that documentation is necessary for the fulfilment of their tasks’ (Article 52(7) CRA).

Augmenting the legislative framework are numerous ‘soft law’ instruments (recommendations, guidelines and the like) published by ENISA, the EDPB and international industry standards-setting bodies. Several sets of guidelines from the EDPB are especially relevant for application of Article 32 GDPR. These include guidelines addressing the need for data security measures in respect of the creation of video surveillance policies and procedures,¹⁸ the manufacturing and operation of connected vehicles,¹⁹ and the use of location data and contact tracing tools during the COVID-19 pandemic.²⁰ The EDPB has also addressed the division of responsibility for data security measures in the context of controller-processor relationships.²¹

2. International instruments

Article 7 of the Council of Europe’s Convention 108 contains a security obligation.²² It provides that ‘appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination’. This provision uses more flexible wording than Article 32 GDPR. It also does not contain the same level of specificity. Convention 108+ contains a similar provision in Article 7(1), stating that ‘[e]ach Party shall provide that the controller, and, where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data’.²³

3. National developments

Article 17 DPD already required EU Member States to impose security obligations on controllers. Post-GDPR, Member States may also implement data security provisions that are more elaborate than Article 32 GDPR. An example is provided by Article 64 of the German Federal Data Protection Act 2017 which was amended to implement certain requirements of the GDPR and contains a detailed list of requirements to ensure the security of data processing.²⁴ The security requirements of the German Act have become influential in practice and are often agreed by parties as the standard for measures required by Article 28 GDPR (requirements for processors) and the EU-approved standard contractual clauses for data transfers. Obviously, though, differing

¹⁷ The CRA is ‘without prejudice’ to the GDPR, ‘including to provisions relating to the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance of processing operations by controllers and processors with that Regulation’ (rec. 32 CRA).

¹⁸ EDPB 2019, pp. 31-32.

¹⁹ EDPB 2020A, paras. 56-57 and 90-91.

²⁰ EDPB 2020B, para. 45.

²¹ EDPB 2020C. See further section C1 in this commentary.

²² Art. 7 Convention 108.

²³ Art. 7(1) Convention 108+.

²⁴ German Federal Data Protection Act 2017.

national legislative rules enacted in response to the GDPR risk undermining the pan-European harmonisation of data security requirements.²⁵

4. Case law

There is so far just one CJEU judgment dealing at length with Article 32: the judgment handed down on 14 December 2023 in the NAP case.²⁶ The case arose in the aftermath of a large-scale hack of personal data stored by the Bulgarian National Revenue Authority (Natsionalna agentsia za prihodite (NAP)). The Bulgarian Supreme Administrative Court requested the CJEU to answer three main questions: (i) whether the data breach creates a presumption that the controller failed to implement the requisite ‘technical and organisational measures’ under Articles 32 and 24; (ii) who bears the burden of proving that the implemented measures are appropriate pursuant to Article 32; and (iii) whether damage that is to be compensated for under Article 82 GDPR may extend to the psychological distress suffered by the data subjects because of their fears over potential misuse of the hacked data even where no evidence has been adduced that the data have been misused or that the data subjects have otherwise been harmed.

The CJEU answered the first question in the negative, stating that a security breach as such will not necessarily constitute a presumption that Article 32 has been infringed; rather, an infringement will only arise if the controller or processor has failed to take the measures required by Article 32 (including documentation of these measures).²⁷ As for the second question, the Court stated that controllers bear the burden of proving that the implemented security measures are appropriate pursuant to Article 32, and that this burden of proof follows from the principle of accountability in Articles 5(2) and 24.²⁸ On the question of damage, the Court answered in the affirmative, but held that the fear must be capable of being verified by a national court as ‘well founded, in the specific circumstances at issue and with regard to the data subject’.²⁹ The judgment is dealt with at greater length in Section C below.

Another relevant CJEU judgment was handed down on 26 September 2024 in the case of *TR v Land Hessen*. The case concerns the remedial actions required of a DPA in the aftermath of a data breach; more specifically, whether a DPA in such a situation must exercise a corrective power, such as issuing an administrative fine pursuant to Articles 58(2)(i) and 83 GDPR. The CJEU decided in the negative, ‘where such action is not appropriate, necessary or proportionate to remedy the shortcoming found and to ensure that that regulation [the GDPR] is fully enforced’.³⁰ The judgment is dealt with at greater length in Section C below.

Of more general importance is case law anchoring security of personal data in the EU’s constitutional framework for fundamental rights protection. In *Digital Rights Ireland*, the CJEU seemed to equate data security with the ‘essence’ of the right to data protection in Article 8 CFREU.³¹ The Court stated:

Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because

²⁵ See Wolters 2017, p. 165.

²⁶ Case C-340/21, *VB v Natsionalna agentsia za prihodite*.

²⁷ *Ibid.*, paras. 29–31.

²⁸ *Ibid.*, paras. 50–52.

²⁹ *Ibid.*, para. 85.

³⁰ Case C-768/21, *TR v Land Hessen*, para. 50.

³¹ Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*.

Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that, without prejudice to the provisions adopted pursuant to Directives 95/46 and 2002/58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data.³²

The Court adopted a similar line in *Opinion 1/15*, finding that the envisaged agreement for transferring passenger name record ('PNR') data to Canada did not 'affect the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter' because it 'lays down ... rules intended to ensure, inter alia, the security, confidentiality and integrity of that data, and to protect it against unlawful access and processing'.³³

There is some ambiguity in *Digital Rights Ireland* and *Opinion 1/15* as to the precise role played by the technical and organisational security measures (as opposed to the legal rules requiring such measures) for ensuring preservation of the essence of the rights concerned. While the existence of the legal requirements is clearly acknowledged by the Court as instrumental for preserving this essence, the status of the measures as such remains less clear.³⁴ This matter is neither clarified nor addressed in the NAP case, where the Court largely avoided drawing upon its fundamental rights jurisprudence.

The ECtHR has also ruled on the adequacy of data security obligations pursuant to Article 8 ECHR on the right to respect for private and family life, home and correspondence. In *Z v Finland*, the Court held that domestic law must afford appropriate safeguards to prevent any communication or disclosure of personal health data as may be inconsistent with Article 8 guarantees.³⁵ Subsequently, the ECtHR ruled directly on security obligations related to processing of health data in *I v Finland*.³⁶ In this case, the Court held that Finland violated its positive obligations to ensure respect for the right laid out in Article 8(1) ECHR by failing to secure a patient's medical data against unauthorised access at a public hospital due to the lack of adequate technical and organisational measures.³⁷ Although Finnish law requires patient data to be kept confidential, this legal requirement was deemed insufficient for the purposes of Article 8 ECHR without extra-legal measures to back it up. The judgment may be viewed as implicitly championing the ideals of 'security by design' and 'data protection by design' through requiring, in effect, a proactive implementation of technical and organisational security measures as an essential part of a state's positive obligations under Article 8(1) ECHR.³⁸

In several later cases, the ECtHR has generally specified 'procedures for preserving the integrity and confidentiality of data and procedures for its destruction' as safeguards required by Article 8(2) ECHR.³⁹ More notable, however, is its judgment in *Podchasov v Russia* concerning the normative status of end-to-end encryption for users of the popular electronic communications service, Telegram. The ECtHR found that national legislation mandating

³² Ibid., para. 40. See further regarding this point Lynskey 2015, p. 271; Bygrave 2021, p. 143–144.

³³ *Opinion 1/15*, paras. 150–151.

³⁴ Porcedda views this ambiguity as contributing to a general 'effacement of technology' from EU technology law: see Porcedda 2023, especially ch. 9.

³⁵ ECtHR, *Z v Finland*, paras. 95–96.

³⁶ ECtHR, *I v Finland*.

³⁷ Ibid., para. 47.

³⁸ See further Bygrave 2021, p. 143.

³⁹ ECtHR, *S and Marper v UK*, para. 99; ECtHR, *PN v Germany*, para. 62.

Telegram to provide law enforcement authorities with decryption capabilities giving ‘backdoor’ access to the encrypted communications of all Telegram users

would affect everyone indiscriminately, including individuals who pose no threat to a legitimate government interest[,] ... make it technically possible to perform routine, general and indiscriminate surveillance of personal electronic communications ... and ... seriously compromise the security of all users’ electronic communications.⁴⁰

With parallels to the CJEU’s judgment in *Digital Rights Ireland*,⁴¹ the Strasbourg Court went on to hold:

In so far as this legislation permits the public authorities to have access, on a generalised basis and without sufficient safeguards, to the content of electronic communications, it *impairs the very essence* of the right to respect for private life under Article 8 of the Convention.⁴²

Case law at national level has also been important in elevating the normative importance of data security in EU law. In a judgment handed down in 2008, the German Federal Constitutional Court recognised a ‘fundamental right to the guarantee of the confidentiality and integrity of information-technology systems’ (‘Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme’) as part of the German Constitution.⁴³ There is evidence to suggest that the judgment helped lift data security into the collection of core data protection principles set out in Article 5 GDPR and helped inspire the line taken by the CJEU in *Digital Rights Ireland*.⁴⁴

C. Analysis

1. Scope of the security obligation

Both data controllers and processors are subject to the data security obligations of Article 32. Beyond the direct obligations placed by Article 32 on controllers, the GDPR makes changes regarding controllers’ engagement of processors. While the DPD only required the controller to impose a contractual security obligation on the processor, Article 32 GDPR directly imposes this obligation on the processor itself. Thus, processors also have a statutory obligation to ensure an appropriate level of security of the processing under the GDPR. In addition, Article 28(4) requires controllers to conclude a written contract with the processor that, among other things, requires the processor to take all measures required by Article 32, as well as to assist the controller in ensuring compliance with its own obligations under Article 32.

From the controller’s perspective, security considerations must be taken into account in the selection of the processor. This was already the case under Article 17(2) DPD which provided that controllers must choose a processor ‘providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out’. Under the GDPR, this provision is replicated in modified form in Article 28(1) in much

⁴⁰ ECtHR, *Podchasov v Russia*, para. 77.

⁴¹ Indeed, the judgment is referenced by the ECtHR as part of background ‘international material’: *ibid.*, para. 31.

⁴² *Ibid.*, para. 80 (emphasis added).

⁴³ Bundesverfassungsgericht, judgment 1 BvR 370/07 and 595/07 of 27 February 2008, para. 166ff.

⁴⁴ See further Bygrave 2021, p. 144–145.

more general terms, which are no longer limited to security, but extend to all GDPR requirements.

Article 28(4) requires the processor to bind sub-processors by a contract containing the ‘same data protection obligations’ as imposed on the processor by the controller, which includes measures related to data security. Article 32(4) also has implications for the use of sub-processors and for employees. Externally, under Article 32(4) controllers and processors must ‘take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data’ (which can include sub-processors) does not process them except on instructions from the controller, unless this is required by EU law or Member State law. This requires the conclusion of written contracts with sub-processors. Internally, both controllers and processors must require their employees — or anyone acting under their authority — to only process personal data under the instructions of the controller (Article 32(4)). In practice, such instructions should reflect the controller’s obligations under Article 32, which means that the security safeguards required by Article 32 must also be made binding internally within each data controller’s or processor’s structure.

Further elaboration of the impact of security requirements on the respective roles of controllers and processors is provided in EDPB Guidelines 7/2020. The Guidelines define decisions on ‘non-essential means’ with regard to security as concerning practical aspects of implementation,⁴⁵ and state that while such decisions could be left to the processor, the controller must stipulate certain elements in the processor contract and be fully informed about the means that are used.⁴⁶ The EDPB also finds it advisable to document at the minimum the necessary technical and organisational measures in the contract.⁴⁷ The Guidelines contain detailed pronouncements on what should be included in the contract with regard to security, including ‘the security measures to be adopted, an obligation on the processor to obtain the controller’s approval before making changes, and a regular review of the security measures so as to ensure their appropriateness with regard to risks, which may evolve over time. The degree of detail of the information as to the security measures to be included in the contract must be such as to enable the controller to assess the appropriateness of the measures pursuant to Article 32(1) GDPR’.⁴⁸

Finally, regarding contract structure, the Guidelines state as follows:

In some cases, the controller may provide a clear and detailed description of the security measures to be implemented. In other cases, the controller may describe the minimum security objectives to be achieved, while requesting the processor to propose implementation of specific security measures. In any event, the controller must provide the processor with a description of the processing activities and security objectives (based on the controller’s risk assessment), as well as approve the measures proposed by the processor. This could be included in an annex to the contract. The controller exercises its decision-making power over the main features of the security measures, be it by explicitly listing the measures or by approving those proposed by the processor.⁴⁹

⁴⁵ EDPB 2020C, para. 38.

⁴⁶ *Ibid.*, para. 39.

⁴⁷ *Ibid.*

⁴⁸ *Ibid.*, para. 123.

⁴⁹ *Ibid.*, para. 124.

2. Compliance with the security obligation

The security obligation imposed by Article 32 GDPR is essentially framed as a requirement for controllers and processors to implement technical and organisational measures appropriate to the risks of the data processing. This involves a two-step risk management process. As a first step, controllers and processors must identify and assess the particular risks presented by the data processing, paying particular attention to risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. The second step involves identifying and implementing security measures to mitigate the risks. As elaborated further below, both steps must be taken already at the time a system for processing personal data is first conceived, and the steps must be repeated after the system becomes operational, to take account of changes in the threat environment.

Article 32(1) formulates ‘risk’ in terms of ‘varying likelihood and severity for the rights and freedoms of natural persons’. The references to ‘likelihood’ and ‘severity’ reflect the traditional, technical conceptualisation of risk as a function of both the probability and degree of harm — a conceptualisation adopted in other EU legislation.⁵⁰ It is most natural to construe risk in this context as connected primarily to possible harm facing individuals in their role as data subjects. This is borne out also by recital 75 GDPR which provides a lengthy, albeit non-exhaustive, list of examples of relevant risks all of which derive from the processing of personal data. However, the risk assessment parameters here should not be exclusively tied to potential harm to the data protection interests of data subjects, nor just to their interests *qua* individuals. The language of Article 32(1) refers to a generic plurality of rights, freedoms and persons. As Article 1(2) GDPR makes clear (see also recitals 2 and 4 GDPR), the Regulation is intended to safeguard more than simply the fundamental right to data protection. Thus, it makes sense to construe Article 32 as mandating an expansive assessment of potential harms to the rights and freedoms of persons, also taking account of their interests as constituents of groups and other collective entities, along with other broader systemic factors, such as the possibility of emergent harm to critical societal infrastructure.⁵¹ Harm in this context is also to be understood comprehensively: it encompasses not just physical or material damage, but also non-material. This is made clear in recital 75 GDPR and confirmed by the CJEU in, *inter alia*, the NAP case.

The word ‘appropriate’ appears not less than three times in Article 32(1): ‘the controller and the processor shall implement *appropriate* technical and organisational measures to ensure a level of security *appropriate* to the risk, including *inter alia* as *appropriate*...’ (emphasis added). This indicates that controllers and processors must identify the situation-specific risks, assess their potential impact having regard to the particular circumstances of the processing, and implement measures to mitigate (at least) those risks that are the most likely to materialise and those whose impact would be the most severe.

The references to ‘appropriateness’ can be seen as a way of expressing the importance of the principle of proportionality — a general principle of EU law — in determining how to ensure data security. A proportionality analysis generally inquires whether the means used to achieve an aim corresponds to the importance of the aim and whether it is necessary for its achievement.⁵² Thus, the use of security measures should be evaluated based on whether they are reasonably likely to achieve their objectives, and on weighing competing interests, i.e.

⁵⁰ See e.g. Art. 3(2) AIA (defining ‘risk’ as a combination of ‘the probability of an occurrence of harm and the severity of that harm’).

⁵¹ For a similar line, see e.g. Papadaki and Stalla-Bourdillon 2023, p. 664.

⁵² Tridimas 2009, p. 139.

assessing the consequences that a measure has on an interest worthy of legal protection (in this case, the security of data processing), and determining whether those consequences are justified in view of the importance of the objective pursued.⁵³

The GDPR provides some guidance on assessing security risks and identifying what security measures may be ‘appropriate’. Article 32(1) lays out a (non-exhaustive) list of criteria to be taken into account, namely: the state of the art; the costs of implementation; the nature, scope, context and purposes of the processing; and the risk of varying likelihood and severity for the rights and freedoms of individuals. Article 32(2) further specifies the major risks to be alerted of in the following terms: ‘In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed’. Thus, this second paragraph impliedly elaborates on the last two criteria of paragraph 1, as it gives examples of the most likely and/or severe risks to be mitigated. These examples show some similarities to the criteria to be used in determining whether to carry out a data protection impact assessment (‘DPIA’) pursuant to Article 35 GDPR, and the WP29 has emphasised the importance of data security in the context of DPIAs.⁵⁴

The reference to ‘state of the art’ in Article 32(1) deserves special attention. The criterion is frequently employed in EU cybersecurity laws,⁵⁵ although its regulatory origins lies in other legislation, most notably the 1985 Product Liability Directive (Council Directive 85/374/EEC).⁵⁶ Surprisingly, the criterion is not formally defined in EU legislation, nor in CJEU jurisprudence, leaving its semantics vague and underdetermined. The *travaux préparatoires* for the legislative instruments employing the criterion are also of little help.

In German jurisprudence, ‘state of the art’ (‘Stand der Technik’) is typically distinguished from the ‘generally accepted rules of technology’ (‘allgemeine anerkannte Regeln der Technik’) on the one hand, and the ‘state of science and technology’ (‘Stand der Wissenschaft und Technik’) on the other, each operating with different degrees of stringency regarding what regulatees must take into account so as to keep up with technological developments. This jurisprudence is anchored in the judgment of the German Federal Constitutional Court in *Kalkar I*,⁵⁷ where the Court placed ‘Stand der Technik’ between the ‘generally accepted rules of technology’, which operate with the least stringent requirements, and the ‘state of science and technology’, which operate with the most stringent. The ‘generally accepted rules of technology’ encompass ‘the prevailing opinion among technical practitioners’ (‘die herrschende Auffassung unter den technischen Praktikern’) as to what measures are practicable and appropriate.⁵⁸ According to the Court, such a criterion risks ‘continuously falling behind any further technical development’ (‘stets hinter einer weiterstrebenden technischen Entwicklung herhinkt’).⁵⁹ In contrast, with the ‘state of the art’ criterion, ‘the legal standard for what is permitted or required is ... shifted to the front of technical development, since general recognition and practical proof

⁵³ Ibid.

⁵⁴ WP29 2017.

⁵⁵ See e.g. Art. 21 NIS2 Directive and Art. 40(1) EEC.

⁵⁶ See Art. 7(e) Product Liability Directive which refers to the ‘state of scientific and technical knowledge’ as a criterion for assessing possible exemption from the Directive’s strict liability regime.

⁵⁷ Bundesverfassungsgericht, decision of 8 August 1978.

⁵⁸ Ibid., 135.

⁵⁹ Ibid., 135.

alone are not decisive for the state of the art'.⁶⁰ As for the 'state of science and technology', that criterion is even more demanding since it necessitates taking precautions 'according to the latest scientific findings' ('nach den neuesten wissenschaftlichen Erkenntnissen') and these precautions are 'not limited by what is currently technically feasible' ('nicht durch das technisch gegenwärtig Machbare begrenzt').⁶¹

The tripartite typology expounded in *Kalkar I* has since been used as a point of inspiration for construing references to the 'state of the art' criterion in EU cybersecurity and data protection legislation.⁶² However, the typology should not be applied slavishly when construing a provision of EU law; to do otherwise fails to respect the constitutional autonomy of the EU legal order. This is not to say that the line taken in *Kalkar I* is irrelevant for construing the 'state of the art' criterion in Article 32 GDPR; it is a legitimate and significant interpretative source, but it is not decisive. This probably explains why the EDPB, when providing guidance on the criterion as employed in Articles 25 and 32 GDPR, carefully states that the *Kalkar* decision 'may provide the foundation for a methodology for an objective definition of the [state of the art] concept'.⁶³ Nonetheless, good grounds exist — both *lex lata* and *lex ferenda* — for construing the criterion as employed in Articles 32 and 25 GDPR similarly to its conceptualisation in *Kalkar I*.⁶⁴ This means that the criterion likely requires security measures to conform not only with the current state of technological advancement, but also with contemporary practices, standards and other norms for technical and organisational management that are generally regarded as offering the best degree of security at the time.⁶⁵ Thus, the extra-legal perceptions of engineers and industry standards-setting bodies as to which technical, operational and organisational standards provide such optimal security are imported into the interpretation and application of Article 32. As 'soft law' norms, these standards are not decisive for understanding or applying Article 32 requirements, but they will inevitably play a significant role as benchmarks for what are deemed 'appropriate' security measures, particularly in the absence of case law from the CJEU.⁶⁶ Indeed, references to them may be found in some of the DPA decisions addressing security breaches.⁶⁷

Determining the appropriate standards will not always be easy. As the German Federal Constitutional Court noted in *Kalkar I*, courts and regulatory authorities 'must enter into the

⁶⁰ Ibid., 135 ('Der rechtliche Maßstab für das Erlaubte oder Gebotene wird hierdurch an die Front der technischen Entwicklung verlagert, da die allgemeine Anerkennung und die praktische Bewährung allein für den Stand der Technik nicht ausschlaggebend sind').

⁶¹ Ibid., 136.

⁶² See e.g. IT Security Association Germany (TeleTrusT) and ENISA 2021; Schmitz 2022; Bartels and Backer 2018; EDPB 2020D.

⁶³ EDPB 2020D, para. 18, fn. 8 (emphasis added). I read 'may' as denoting 'might' rather than a permission.

⁶⁴ See further the commentary on Art. 25 GDPR in this edition.

⁶⁵ See also e.g. IT Security Association Germany (TeleTrusT) and ENISA 2021, p. 11 ('The "state of the art" refers to the best performance of an IT security measure available on the market to achieve the legal IT security objective'); Bartels and Backer 2018, p. 216 ('Auf den technischen Datenschutz angewendet, bezeichnet der Stand der Technik die am Markt verfügbare Bestleistung einer Maßnahme oder eines Maßnahmenbündels zur Erreichung eines gesetzlichen IT-Sicherheitsziel').

⁶⁶ See further Porcedda 2023.

⁶⁷ See e.g. the decision by the Irish Data Protection Commissioner (DPC) of 15 March 2022 in Case IN 18-11-5 fining Meta Platforms Ireland Ltd. for breach of Arts. 5(2) and 24(1) GDPR, and the Penalty Notice issued in October 2020 by the UK Information Commissioner's Office (ICO) fining Marriott International Inc. for breach of Arts. 5(1)(f) and 32 GDPR. The DPC referred to 'published expert guidance' from ENISA, the US National Institute for Standards and Technology (NIST), and the International Organization for Standardization (ISO) as relevant benchmarks for determining the kinds of security measures required by the GDPR: see DPC Fine, para. 74. As for the ICO, it used guidance documents from the UK National Cyber Security Agency and NIST as relevant benchmarks: see UK ICO Marriott Penalty, paras. 6.15-6.17, 6.20, 6.33, 6.35 and 6.41.

technicians' disagreements to determine what is technically necessary, suitable, appropriate and avoidable' ('müssen in die Meinungsstreitigkeiten der Techniker eintreten, um zu ermitteln, was technisch notwendig, geeignet, angemessen und vermeidbar ist').⁶⁸ Disagreement combined with vagueness over what constitutes the relevant state of the art may also be exploited by regulatees who want to cut compliance costs — a situation that can result in 'cartels of silence'.⁶⁹

Despite such challenges, it is clear that 'state of the art' is a dynamic, fluid criterion necessitating regular revisiting of security practices. In the words of the EDPB, the criterion is 'a dynamic concept that cannot be statically defined at a fixed point in time but should be assessed continuously'.⁷⁰ This line is reinforced in Article 32(1)(d) GDPR which lists as one of four appropriate security measures a 'process for regularly testing, assessing and evaluating the effectiveness' of these measures.

Current technical-managerial standards that may be considered 'state of the art' — such as those of ENISA, the ISO and IEC (International Electrotechnical Commission) — take the same line, pitching security risk management as a proactive, recurrent process.⁷¹ In other words, risk assessment must be first conducted at the stage when a system for processing personal data is being conceived, not when a system is already established. Further, risk management must not be conducted as a one-off step but as an iterative, continually evolving process that takes due account of changes to the threat landscape.⁷²

Implicit in this approach lies the ideal of 'security by design', which, generally speaking, 'exhorts software engineers and others involved in building information systems (IS) architecture to think about the security needs for that architecture before it is built and embed those needs in the architecture's subsequent design and construction'.⁷³ In the present context, security by design is more than a mere ideal; it is a fully-fledged regulatory principle of EU data protection law, with roots in EU primary law in addition to the GDPR and other secondary law.⁷⁴ Its status as a core data protection principle is buttressed by Article 5(1)(f) GDPR, which also embraces, in effect, a design-based approach. The 'by design' element implicit in Article 32 underscores that the provision may be regarded as an offshoot of the general 'data protection by design and by default' requirements of Article 25 GDPR, along with the accountability requirements of Articles 5(2) and 24(1) GDPR. Article 32 should accordingly be read in light of these requirements.

The CJEU's decision in the NAP case falls short of explicitly highlighting the 'by design' element of Article 32. However, it does not reject or otherwise weaken that element, and it

⁶⁸ Bundesverfassungsgericht, decision of 8 August 1978, 136.

⁶⁹ See further Grafenstein 2022, 414, 419 and references cited therein.

⁷⁰ EDPB 2020, para. 20. See also e.g. Schmitz 2022, p. 30.

⁷¹ See e.g. ISO/IEC 2013, clause 0.1 ('It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls'). See also *ibid.*, Annex A, Table A.1 (sections A.14.1 and A.14.2). Cf. ISO 2018, clause 4 ('Risk management anticipates, detects, acknowledges and responds to ... [risks] in an appropriate and timely manner').

⁷² *Ibid.*, clause 10.2 ('The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system').

⁷³ Bygrave 2021, p. 126. See further *ibid.*, pp. 135–36, 142.

⁷⁴ *Ibid.* 'Security by design' mandates also figure strongly in the CRA's 'essential cybersecurity requirements': see Part I Annex I CRA.

goes a long way in pushing for a strong proactive security culture amongst controllers. In the words of the Court,

since the level of protection provided for by the GDPR is dependent on the security measures adopted by controllers of personal data, those controllers *must be encouraged to do everything in their power to prevent* the occurrence of processing operations that do not comply with that regulation, given that they bear the burden of demonstrating the appropriateness of those measures.⁷⁵

Such a culture is fully aligned with the ‘security by design’ and ‘data protection by design’ principles.

The GDPR does not require the use of any particular technology or technical standard for data security.⁷⁶ This is also the case with EU primary law. In the NAP case,⁷⁷ the CJEU provided precious little detail on the actual security measures required by Article 32, and it omitted reference to requirements potentially flowing from the Charter. However, Article 32(1) lists four types of measures as examples of what controllers and processors should implement ‘as appropriate’: the pseudonymisation and encryption of personal data (Article 32(1)(a)); the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems (Article 32(1)(b)); the ability to restore the availability and access to personal data in a timely manner in case of an incident (Article 32(1)(c)); and a process for regularly testing, assessing and evaluating the effectiveness of security measures (Article 32(1)(d)). The second- and third-listed of these measures ought really to be labelled ‘capabilities’ as they do not constitute measures in the sense of intentional actions.

While Article 32 pitches the four examples as not necessarily obligatory in all contexts, it expresses a clear preference for them, making it likely that regulators will expect controllers and processors to use them whenever possible.⁷⁸ Indeed, all of them are arguably so fundamental for ensuring robust security in line with the ‘state of the art’ that envisaging contexts in which they would not be appropriate is extremely difficult. At the same time, their relatively generic formulation as examples — packed within another relatively generic formulation (‘technical and organisational measures’) — allows Article 32 to harbour a potentially large variety of measures (and capabilities) that are to be applied in a flexible, dynamic manner in line with changing threat scenarios.⁷⁹

Augmenting this expansiveness is the explicit mention of ‘organisational’ measures in addition to the merely technical.⁸⁰ Organisational measures primarily concern the assignment and management of roles, duties or tasks, usually within the aegis of a collective entity (e.g. corporation or state agency). Obvious examples in point are security incident response management, staff training on security procedures, and managerial decisions allocating formal responsibility for security-related initiatives. Yet, the open-textured nature of the term ‘organisational’ arguably signals an intention to cover any measure that appreciably bolsters security, even if the measure does not fit snugly within the term’s ordinary literal meaning.

⁷⁵ Case C-340/21, *VB v Natsionalna agentsia za prihodite*, para. 55 (emphasis added).

⁷⁶ See rec. 15 GDPR, explaining that ‘the protection of natural persons should be technologically neutral and should not depend on the techniques used’.

⁷⁷ Case C-340/21, *VB v Natsionalna agentsia za prihodite*.

⁷⁸ For a concise elaboration of what these measures entail, see Papadaki and Stalla-Bourdillon 2023, p. 665–668.

⁷⁹ See also Bygrave 2021, p. 165; Schartum 2021, p. 295.

⁸⁰ Further on their interrelationship, see the commentary on Art. 25 in this edition.

This would be the case, for instance, with particular economic measures (e.g. budgeting for security spending) or legal measures (e.g. drafting contractual terms for the use of computing services).⁸¹

3. Accountability, liability and fines

While both controllers and processors must abide by the requirements of Article 32, the responsibility of controllers is more pronounced. Controllers are subject to the accountability principle enshrined in Article 5(2) (and secondarily in Article 24), which includes the obligation to demonstrate that they ensure appropriate security. The reach of this obligation was brought out in the NAP case, with the CJEU holding that controllers bear the burden of proving that the security measures they implement are appropriate pursuant to Article 32.⁸² Concomitantly, a controller cannot escape damages liability under Article 82 GDPR simply because a third party has carried out a hack; a controller will only escape such liability if it can show that the damage from the breach was ‘in no way’ caused by its own actions (or lack of actions).⁸³ The GDPR does not explicitly impose this accountability obligation on processors, although they are subject to a number of legal requirements, particularly under Article 28.

Article 32(3) provides that controllers and processors may demonstrate compliance with data security requirements by adhering to an approved code of conduct or an approved certification mechanism regarding the security of processing.⁸⁴ The conditions for and the consequences of this are to be determined under Article 40 (for codes of conduct) and Article 42 (for certification mechanisms). It bears emphasis that adherence to either type of instrument will not be decisive for demonstrating compliance; adherence is simply a possible ‘element’ to this end.⁸⁵ Although codes of conduct have been part of the European data protection ‘toolkit’ for many years, their use remains extremely modest.⁸⁶ There are currently only two approved transnational codes (for respectively cloud service providers and cloud infrastructure providers) and only 11 national codes in just five jurisdictions (Italy, Spain, Germany, Belgium and the Netherlands).⁸⁷ In other words, codes of conduct still play a minor role. The same can be said for certification schemes: these are currently operating in only three jurisdictions (Luxembourg, Germany and the Netherlands).⁸⁸

Compensation and liability for violations of Article 32 can be imposed under Article 82 GDPR. Regarding administrative fines under Article 83 GDPR, the amount of such fines is supposed to give due regard to ‘the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32’ (Article 83(2)(d)).

It must be remembered, however, that Article 32 only imposes an obligation of means,⁸⁹ not an obligation to provide a result. This was confirmed by the CJEU in the NAP case.⁹⁰ In other

⁸¹ See further Bygrave 2021, p. 166.

⁸² Case C-340/21, *VB v Natsionalna agentsia za prihodite*, paras. 52-53.

⁸³ *Ibid.*, paras. 71-74.

⁸⁴ See also Art. 24(3) GDPR in respect of controllers.

⁸⁵ See also Papadaki and Stalla-Bourdillon 2023, p. 669.

⁸⁶ See generally Vander Maelen 2023.

⁸⁷ See EDPB Overview. See further the commentary on Art. 40 GDPR in this edition.

⁸⁸ See further the commentary on Art. 42 GDPR in this edition.

⁸⁹ Wolters 2017, p. 172.

⁹⁰ Case C-340/21, *VB v Natsionalna agentsia za prihodite*, paras. 29-31.

words, if a data breach occurs despite the implementation of appropriate security measures, there may still not be an infringement of the GDPR.

The NAP judgment opens up for the possibility of damages liability under Article 82 extending to the psychological distress suffered by data subjects because of their fears over potential misuse of the hacked data in the future, even where no evidence has been adduced that the data have been misused or that the data subjects have otherwise been harmed. However, the CJEU introduces an important qualification in that the fear must be capable of being verified by a national court as ‘well founded’.⁹¹ This tempers the ‘subjective’ with a thick wedge of objectivity.

Fines for violations of Article 32 can range up to € 10 million or 2 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83(4)(a)). Yet, security breaches may attract a higher tier level of administrative fines if they are regarded as breaches of Article 5(1)(f) GDPR. Fine levels are doubled when there is a breach of ‘the basic principles for processing’ under Article 5 (Article 83(5) GDPR). This creates a concurrently applicable two-tiered system for the maximum amount payable in the case of security breaches. The system has been characterised as ‘intriguing, albeit confusing’.⁹² The arcane and inconsistent way in which DPAs have implemented the system has exacerbated the confusion.⁹³ It seems sensible to operationalise the system such that ‘the higher level of fine may (and ought to) be applied in cases of egregious or especially negligent behaviour on the part of controllers; the lower tier being reserved for other cases’.⁹⁴

The possibility of other security-related sanctions applying should be kept in mind. For instance, a separate sanction may apply if there is a failure to notify a data breach to the DPA or affected individuals in accordance with Articles 33 and 34 GDPR. As noted by the WP29 in its guidance on data breach notification under the GDPR,⁹⁵ the latter type of sanction is distinct from a sanction for absence of appropriate security measures.⁹⁶ Another example is the possibility of a separate sanction for failing to document that appropriate security measures have been implemented. Such a sanction would flow from breach of the documentation requirements inherent in the principle of accountability under Articles 5(2) and 24(1) GDPR.⁹⁷

It has been stated that the imposition of *criminal* sanctions for violation of Article 32 could violate the principle of legality because its requirements are formulated in vague and general terms.⁹⁸ This was the reason that the Italian legislature decided not to provide for criminal sanctions for violation of security requirements under the GDPR.⁹⁹

Nonetheless, *civil* liability for breaches of data security is potentially massive. DPAs have issued large fines for such breaches. For example, in October 2020, the UK Information Commissioner (ICO) imposed a penalty of £20 million on British Airways (BA).¹⁰⁰ The breach involved an attacker gaining access to BA’s IT systems and accessing card data. The ICO also found that BA

⁹¹ Ibid., para. 85.

⁹² Bygrave 2021, p. 169-170.

⁹³ Ibid., p. 170.

⁹⁴ Ibid.

⁹⁵ WP29 2018, p. 10.

⁹⁶ Ibid., p. 8.

⁹⁷ See DPC Fine (elaborated further below) for an instance of such a sanction being imposed.

⁹⁸ Tosoni 2018, p. 1200.

⁹⁹ Ibid.

¹⁰⁰ UK ICO British Airways Penalty.

was in breach of its own security policies. Another example is the fine of € 2.25 million imposed by the CNIL in November 2020 on Carrefour France for a security breach, which included not taking the necessary measures to secure personal data on the company's website even though it knew it had a vulnerability.¹⁰¹ Also noteworthy is the fine of € 17 million imposed by the Irish Data Protection Commissioner in March 2022 on Meta Platforms Ireland (formerly Facebook Ireland). The latter fine was not grounded in breach of Articles 32 or 5(1)(f), but the corporation's failure *to document* that it had instituted appropriate security measures — a failure incurring breach of Articles 5(2) and 24(1) GDPR.¹⁰²

In the aforementioned case of *TR v Land Hessen*, the CJEU made it clear that, as a legal point of departure, a DPA is not required to issue a fine in the aftermath of a data security breach.¹⁰³ Here, the Court also referenced recital 148 GDPR which indicates that a fine need not be imposed for minor infringements or in cases when imposition would constitute a disproportionate burden to a natural person.¹⁰⁴ Concomitantly, a complainant whose rights have been infringed as a result of the breach does not have an absolute subjective right 'to seek the imposition by the supervisory authority of an administrative fine on the controller'.¹⁰⁵ The judgment thereby provides a DPA with some discretion as to how it reacts to evidence of the breach. However, this room for discretion is bounded by a DPA's overarching obligation 'to react appropriately in order to remedy the shortcoming found'.¹⁰⁶ Reacting appropriately entails ensuring full enforcement of the GDPR and 'a consistent and high level of protection of personal data through strong enforcement of the rules'.¹⁰⁷ The CJEU intimates that the non-exercise of corrective powers will occur on an exceptional basis — e.g. in a situation in which infringement of the GDPR 'has already been made good and ... the processing of personal data by the controller thereof in compliance with that regulation is ensured, and ... such non-exercise on the part of the supervisory authority is not liable to undermine the requirement of strong enforcement of the rules'.¹⁰⁸

4. Security measures in the context of other obligations imposed by the GDPR

References to the obligation to ensure appropriate security measures are made throughout the GDPR. For instance, data processing for the purpose of ensuring network and information security, such as to prevent data breaches, constitutes a legitimate interest of the controller and does not require reliance on any other legal ground for processing (recital 49). Another example is that, whenever possible, controllers and processors must include a general description of the technical and organisational security measures in their records of processing activities (Articles 30(1)(g) and 30(2)(d)). Security measures are also important in the context of Binding Corporate Rules ('BCRs'), when an organisation wishes to obtain regulatory approval of them (Article 47(2)(d)).

¹⁰¹ CNIL Carrefour Fine.

¹⁰² DPC Fine, para. 130 ('the fundamental concern arising in this Inquiry is FB-I's [Facebook Ireland's] failure to have in place appropriate technical and organisational measures such as would enable it *to readily demonstrate* the security measures that it implemented in practice to protect EU users' data' [emphasis added]).

¹⁰³ Case C-768/21, *TR v Land Hessen*, para. 50.

¹⁰⁴ *Ibid.*, para. 47.

¹⁰⁵ *Ibid.*, para. 41.

¹⁰⁶ *Ibid.*

¹⁰⁷ *Ibid.*, para. 40.

¹⁰⁸ *Ibid.*, para. 46; see also para. 43.

Select Bibliography

International instruments

Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS No. 108.

Convention 108+: Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data 2018, CM/Inf(2018)15-final.

EU legislation

AIA: Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L 2024/1689, 12.7.2024.

CRA: Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) [2024] OJ L 2024/2847.

Cybersecurity Act: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ 2019 L 151/15.

Digital Operational Resilience Act: Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, OJ 2022 L 333/1.

DORA: Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, OJ L 333/1.

EECC: Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), OJ 2018 L 321/36.

GDPR: 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) (Text with EEA relevance), OJ 2016 L 119/1.

Medical Devices Regulation: Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L 117/1.

NIS Directive: Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ 2016 L 194/1.

NIS2 Directive: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, OJ 2022 L 133/80.

Product Liability Directive: Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (Product Liability Directive) [1985] OJ L 210/29.

PSD2 Directive: Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC, OJ 2015 L 337/35.

National legislation

Belgian Data Protection Law 1992: Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, van 8 december 1992; Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, du 8 décembre 1992) (repealed).

German Federal Data Protection Act 2017: Bundesdatenschutzgesetz vom 30. Juni 2017, BGBl. 2017 Teil I Nr. 2097.

Academic writings

Bartels and Backer 2018: Bartels and Backer, 'Die Berücksichtigung des Stands der Technik in der DSGVO: Neue Anforderungen an die IT-Sicherheit im Datenschutz', 4 *Datenschutz und Datensicherheit* (2018), 214.

Bygrave 2021: Bygrave, 'Security by Design: Aspirations and Realities in a Regulatory Context', 8(3) *Oslo Law Review* (2021), 126.

Bygrave 2025: Bygrave, 'The Emergence of EU Cybersecurity Law: A Tale of Lemons, Angst, Turf, Surf and Grey Boxes', 56 *Computer Law & Security Review* (2025), 106071.

Grafenstein 2022: Grafenstein, 'Co-regulation and the competitive advantage in the GDPR: data protection certification mechanisms, codes of conduct and the 'state of the art' of data protection-by-design', in González Fuster, van Brakel, and de Hert (eds.), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Edward Elgar 2022), 398.

Hermann and Pridöhl 2020: Hermann and Pridöhl, 'Basic Concepts and Models of Cybersecurity', in Christen, Gordijn and Loi (eds.), *The Ethics of Cybersecurity* (Springer 2020), 11.

Lynskey 2015: Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015).

Markou 2023: Markou, 'Article 29', in Kosta and Boehm (eds.), *The EU Law Enforcement Directive (LED): A Commentary* (OUP 2023), 461.

Papadaki and Stalla-Bourdillon 2023: Papadaki and Stalla-Bourdillon, 'Article 32', in Spiecker genannt Döhmann, Papakonstantinou, Hornung and de Hert (eds.), *General Data Protection Regulation: Article-by-Article Commentary* (Nomos/Beck/Hart 2023), 659.

Porcedda 2023: Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis* (Hart 2023).

Schartum 2021: Schartum, "'Technical and Organisational Measures"—A Systematic Analysis of Required Data Protection Measures in the GDPR', in Herveg (ed.), *Deep Diving into Data Protection: 1979-2019 : Celebrating 40 Years of Research on Privacy and Data Protection at the CRIDS* (Larcier 2021), 289.

Schmitz 2022: Schmitz, 'Conceptualising the Legal Notion of "State of the Art" in the Context of IT Security', in Friedewald and others (eds.), *Privacy and Identity Management: Between Data Protection and Security* (Springer 2022), 25.

Tosoni 2018: Tosoni, 'Rethinking Privacy in the Council of Europe's Convention on Cybercrime', 34(6) *Computer Law & Security Review* (2018), 1197.

Tridimas 2009: Tridimas, *The General Principles of EU Law* (2nd edn, OUP 2009).

Vander Maelen 2023: Vander Maelen, *Don't Count Your Codes Before They Hatch: A Theoretical and Empirical Analysis of Codes of Conduct under the General Data Protection Regulation* (Dissertation Ghent University, 2023).

Wolters 2017: Wolters, 'The Security of Personal Data under the GDPR: A Harmonized Duty or a Shared Responsibility?', 7 *International Data Privacy Law* (2017), 165.

Papers of data protection authorities

EDPB 2018: European Data Protection Board, ‘Endorsement 1/2018’ (25 May 2018).

EDPB 2019: European Data Protection Board, ‘Guidelines 3/2019 on the processing of personal data through video devices’ (29 January 2020).

EPDB 2020A: European Data Protection Board, ‘Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications’ (28 January 2020).

EDPB 2020B: European Data Protection Board, ‘Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak’ (21 April 2020).

EDPB 2020C: European Data Protection Board, ‘Guidelines 07/2020 on the concepts of controller and processor in the GDPR’ (2 September 2020).

EDPB 2020D: European Data Protection Board, ‘Guidelines 4/2019 on Article 25: Data Protection by Design and by Default’ (20 October 2020).

WP29 2017: Article 29 Working Party, ‘Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is “Likely to Result in a High Risk” for the Purposes of Regulation 2016/679’ (WP 248 rev.01, as last revised and adopted on 4 October 2017).

WP29 2018: Article 29 Working Party, ‘Guidelines on Personal Data Breach Notification under Regulation 2016/679’ (WP 250 rev.01, as last revised and adopted on 6 February 2018).

CNIL Carrefour Fine: CNIL, ‘Délibération de la formation restreinte n° SAN-2020-008 du 18 novembre 2020 concernant la société CARREFOUR France’.

DPC Fine: Irish Data Protection Commissioner, ‘Decision of 15 March 2022 in Case IN 18-11-5 regarding Meta Platforms Ireland Ltd’.

UK ICO British Airways Penalty: UK Information Commissioner, Penalty Notice, British Airways plc, COM0783542, 16 October 2020.

UK ICO Marriott Penalty: UK Information Commissioner, Penalty Notice, Marriott International Inc, COM0804337, 30 October 2020.

Reports and recommendations

ENISA Report: European Union Agency for Network and Information Security, ‘ENISA’s Role in the European Digital Single Market (DSM)’ (2018), available at <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa2019s-role-in-the-european-digital-single-market-dsm>.

ISO 2018: ISO 31000:2018 standard (Risk management – Guidelines).

ISO/IEC 2013: ISO/IEC 27001:2013 standard (Information technology – Security techniques – Information security management systems – Requirements).

ISO/IEC 2018: ISO/IEC 27000:2018(E) standard (Information technology – Security techniques – Information security management systems – Requirements).

IT Security Association Germany (TeleTrusT) and ENISA, ‘IT Security Act (Germany) and EU General Data Protection Regulation: Guideline “State of the Art” – Technical and Organisational Measures’ (version 1.9_2021-09 EN).

Others

EDPB Overview, ‘Codes of Conduct, amendments and extensions’, available at https://www.edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en?f%5B0%5D=coc_scope%3Anational&page=0.

Article 45. Transfers on the basis of an adequacy decision

*CHRISTOPHER KUNER AND LAURA DRECHSLER**

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.
2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
 - (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
 - (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
 - (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.
3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).
4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted

* This contribution is based on the first edition of the Commentary in which Christopher Kuner authored the contribution on Art. 45.

pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2). On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).
6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.
7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.
8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.
9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

Relevant Recitals

(102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.

(103) The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.

(104) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security,

defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

(105) Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.

(106) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organisation, and monitor the functioning of decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council as established under this Regulation, to the European Parliament and to the Council.

(107) The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

CLOSELY RELATED PROVISIONS

Recital 6; recital 102; Articles 13(1)(f) and 14(1)(f) (Information to a data subject); Article 15(1)(c) (Right to access information about data recipients in third countries); Article 23(2)(d) (Member States can restrict individuals' rights but must provide for safeguards to prevent abuse or unlawful transfer) (see too recital 153);

Article 28(3)(a) (Provisions of a data processing agreement stipulating controller's instructions regarding data transfers); Article 30(1)(e) and (2)(c) (Internal records about data transfers); Article 40(2)(j) (Data transfer codes of conduct); Article 44 (General principles for transfers); Article 70(1)(s) (Assessment by the Board of the level of protection in a third country); Article 83(5)(c) (Fines for non-compliance with data transfer restrictions); Article 96 (Relationship with previously concluded agreements of the EU Member States)

RELEVANT CASE LAW

CJEU

Case C-101/01, *Criminal proceedings against Bodil Lindqvist*, judgment of 6 November 2003 (ECLI:EU:C:2003:596).

Joined Cases C-317/04 and C-318/04, *European Parliament v Council of the European Union and Commission of the European Communities*, judgment of 30 May 2006 (Grand Chamber) (ECLI:EU:C:2006:346).

Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, judgment of 8 April 2014 (Grand Chamber) (ECLI:EU:C:2014:238).

Case C-362/14, *Maximilian Schrems v Data Protection Commissioner*, judgment of 6 October 2015 (Grand Chamber) (ECLI:EU:C:2015:650) ('Schrems I').

Opinion of Advocate General Bot in Case 362/14, *Maximilian Schrems v Data Protection Commissioner*, delivered on 23 September 2015 (ECLI:EU:C:2015:650).

Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for Home Department v Tom Watson and Others*, judgment of 21 December 2016 (Grand Chamber) (ECLI:EU:C:2016:970).

Opinion 1/15, Opinion of 26 July 2017 (Grand Chamber) (ECLI:EU:C:2017:592).

Opinion of Advocate General Mengozzi in *Opinion 1/15*, delivered on 8 September 2016 (ECLI:EU:C:2016:656).

Case T-670/16, *Digital Rights Ireland Ltd v European Commission*, GC, order of 22 November 2017 (ECLI:EU:T:2017:838).

Opinion of Advocate General Saugmandsgaard Øe in Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems*, delivered on 19 December 2019 (ECLI:EU:C:2019:1145).

Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems*, judgment of 16 July 2020 (Grand Chamber) (ECLI:EU:C:2020:559) ('Schrems II').

Case T-553/23 R, *Phillipe Latombe v European Commission* (pending).

Case T-325/23, *Meta Platforms Ireland v EDPB* (pending).

ECtHR

Big Brother Watch and Others v United Kingdom, Appl. Nos. 58170/13, 62322/14, and 24960/15, judgment of 25 May 2021 (Grand Chamber).

Centrum for Rättvisva v Sweden, Appl. No. 35252/08, judgment of 25 May 2021 (Grand Chamber).

Association confraternelle de la presse judiciaire v France, Appl. No. 49526/15, decision of 10 December 2024.

Germany

German Federal Constitutional Court (*Bundesverfassungsgericht*), judgment 1 BvR 966/09 of 20 April 2016, BVerfGE 141, 220.

German Regional Court of Traunstein (*Landesgericht Traunstein*), final judgment of 8 July 2024, 9 O 173/24.

Ireland

Schrems v Data Protection Commissioner [2014] IEHC 310, [2014] 2 ILRM 441.

Schrems v Data Protection Commissioner (No. 2) [2014] IEHC 351, [2014] 2 ILRM 506.

Data Protection Commissioner and Facebook Ireland Limited and Maximilian Schrems, Irish High Court, 2016 No. 4809 P, 3 October 2017.

A. Rationale and Policy Underpinnings

Article 45 GDPR sets forth the procedure and standards for determining when the Commission may issue a decision finding that third countries (including territories or one or more specified sectors within such countries) and international organisations provide an adequate level of data protection.

Chapter V of the GDPR creates a three-tiered structure for legal bases for international data transfers, with adequacy decisions at the top, appropriate safeguards in the middle and derogations at the bottom. An adequacy decision requires that the legal system of a third country or international organisation be ‘essentially equivalent’ to that of EU data protection law. When there is no adequacy, appropriate safeguards may be used;¹ the CJEU has ruled that appropriate safeguards must also provide an essentially equivalent level of data protection.² Finally, derogations may also be used under certain conditions.³

Adequacy requires both that the content of data protection rules in third countries or international organisations meet the standards of EU law, and that such rules be effective in practice.⁴ It is not required that the rules be identical to those of the EU; rather, they must be ‘essentially equivalent’ to EU rules. As the WP29 stated,⁵ this means that they must comply with a ‘core’ of principles relating both to the content of data protection rules and their enforcement, based on the GDPR, the Charter of Fundamental Rights of the European Union (‘CFR’) and other relevant international instruments, such as Council of Europe Convention 108+. This also requires that attention be paid to the legal framework for the access of public authorities to personal data (‘governmental access’).⁶

Article 45 specifically deals with the issuance of Commission decisions on adequacy. The criteria of Article 45 can be relevant in determining the level of protection in other situations as well, for example for determining the required level of protection for appropriate safeguards,⁷ but the Article does not create the possibility of determining adequacy outside the context of a formal Commission decision (for example, parties that transfer data cannot determine adequacy by themselves).

B. Legal Background

1. EU legislation

Article 25 DPD contained rules concerning the adequacy of protection in third countries. The following are the main differences between Article 25 DPD and Article 45 GDPR:

1. Article 25 required an adequate level of protection in a third country to which personal data are transferred, while Article 45 sets out an adequate level of protection in a third country or international organisation as one option under which personal data may be transferred which has to be interpreted in light of the CJEU’s case law on essential equivalence.⁸

¹ See the commentary on Art. 46 in this edition.

² Case C-311/18, *Schrems II*, para. 105.

³ See the commentary on Art. 49 in this edition.

⁴ WP29 2018, p. 3.

⁵ Ibid.

⁶ Ibid., p. 4. See also WP29 2016.

⁷ See EDPB 2021C, p. 16.

⁸ Case C-362/14, *Schrems I*; Case C-311/18, *Schrems II*.

2. Article 45(2) contains a more detailed and exhaustive list of conditions for adequacy than what was contained in Article 25.
3. Article 45 does not allow the Commission to find that a third country does *not* provide an adequate level of data protection (a so-called ‘negative adequacy decision’), a possibility that was provided in Article 25(4) DPD. However, the removal of this possibility is only relevant with regard to third countries for which no adequacy decision is in force, since the Commission may repeal, amend or suspend adequacy decisions that are in force under Article 45(5) GDPR.
4. Article 45 provides only for EU adequacy decisions, whereas Article 25 also mentioned decisions of the Member States.
5. Article 45 also mentions adequacy decisions covering transfers to international organisations, specific sectors or territories of a third country, whereas Article 25 referred solely to transfers to third countries.
6. Article 45 requires a periodic review of adequacy decisions at least every four years.

At the time of writing, there are fifteen Commission adequacy decisions issued under the GDPR, covering the following countries: Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, the Republic of Korea, New Zealand, Switzerland, the United Kingdom, Uruguay, and the United States.⁹ An adequacy decision may cover all data transfers to a third country that fall under the GDPR, or only some of them. The Commission has stated its intention to issue further adequacy decisions.¹⁰ In 2012, the WP29 found that the Principality of Monaco guaranteed an adequate level of protection under Article 25(6) DPD.¹¹ However, a Commission adequacy decision was never issued, and thus data transfers to Monaco are subject to the same restrictions as those to any other third country.

The LED contains an analogous provision (Article 36) allowing the Commission to declare that third countries, territories within a third country, or international organisations provide adequate protection for data transfers in the law enforcement sphere.¹² So far, only one such decision has been issued, covering the United Kingdom.¹³

Three former adequacy decisions are no longer in force after the data transfer mechanisms upon which they were based were invalidated, i.e. the 2004 decision on the transfer of passenger name record (‘PNR’) data to the United States’ Bureau of Customs and Border Protection¹⁴ which was invalidated by the CJEU;¹⁵ the 2000 decision on the EU-US Safe Harbour arrangement¹⁶ which the CJEU invalidated in its *Schrems I*¹⁷ judgment in 2015; and

⁹ See Commission Decision Andorra 2010; Commission Decision Argentina 2003; Commission Decision PIPEDA 2002; Commission Decision Faroe Islands 2010; Commission Decision Guernsey 2003; Commission Decision Israel 2011; Commission Decision Isle of Man 2004; Commission Decision Japan 2019; Commission Decision Jersey 2008; Commission Decision Korea 2021; Commission Decision New Zealand 2013; Commission Decision Switzerland 2000; Commission Decision UK GDPR; Commission Decision Uruguay 2012; and Commission Decision EU-US Data Privacy Framework. The UK has also received an adequacy decision under the LED. See Commission Decision UK LED.

¹⁰ EC Communication 2020, p. 17.

¹¹ WP29 2012, p. 19.

¹² See Drechsler 2024.

¹³ Commission Decision UK LED.

¹⁴ Commission Decision US 2004.

¹⁵ Joined Cases C-317/04 and C-318/04, *Parliament v Council and Commission*. Regarding this judgment, see Docksey 2014, pp. 100–106.

¹⁶ Safe Harbour 2000.

¹⁷ Case C-362/14, *Schrems I*.

the EU-US Privacy Shield¹⁸ which the CJEU invalidated in 2020 in its *Schrems II* judgment.¹⁹ In addition, the adequacy decision issued in 2005 covering the transfer of PNR data of air passengers to the Canada Border Services Agency expired in 2009.²⁰

In December 2016, the Commission issued a decision that amended eleven existing adequacy decisions to take into account the requirements of the *Schrems I* judgment.²¹ The decision amends the adequacy decisions covering Andorra, Argentina, the Canadian Personal Information Protection and Electronic Documents Act, the Faeroese Act on the processing of personal data, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. It makes changes to each decision that require Member State data protection authorities to inform the Commission when they take decisions to suspend or ban data flows; require the Commission to monitor developments in the respective third country that could affect the functioning of the decision; order the Commission and the Member States to keep each other informed about cases where the action of bodies in the third country responsible for ensuring compliance fail to do so; obligate the Member States and the Commission to inform each other of indications that interferences by public authorities responsible for national security, law enforcement or other public interests go beyond what is strictly necessary or that there is no effective legal protection against such interferences; and require the Commission to inform the competent authorities of the third country and to propose draft measures to repeal or suspend the decision or limit its scope when evidence shows that an adequate level of protection is no longer ensured.

In January 2017, the Commission announced that it will ‘actively engage with key trading partners in East and South-East Asia, starting from Japan and Korea in 2017, and, depending on progress towards the modernisation of its data protection laws, with India, but also with countries in Latin America, in particular Mercosur, and the European neighbourhood which have expressed an interest in obtaining an “adequacy finding”’.²² In its 2024 evaluation of the GDPR, the Commission mentions Kenya, Brazil and the European Patent Organisation as targets for adequacy decisions,²³ but it is not clear how far the negotiations for each have advanced or even started.²⁴ It also notes ongoing talks with Japan to extend the adequacy decision beyond the commercial organisations it is currently limited to.²⁵

2. International instruments

In *Opinion 1/15*, the Court of Justice of the EU found that the transfer of personal data may be legalised by an international agreement.²⁶ Such agreements must meet the *Schrems* standard of ‘essential equivalence’ with EU law,²⁷ and must also fulfil the requirements of EU primary law, in particular the Charter. The GDPR does not further specify the conditions under which international agreements may provide a legal basis to transfer personal data, beyond stating in recital 102 that the GDPR is ‘without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate

¹⁸ Commission Decision Privacy Shield 2016.

¹⁹ Case C-311/18, *Schrems II*.

²⁰ Commission Decision Canada 2006, Art. 7.

²¹ Commission Decision 2016/2295.

²² EC Communication 2017, p. 9.

²³ EC Communication 2024, p. 21.

²⁴ Czerniawski 2024, p. 229.

²⁵ EC Communication 2024, p. 22.

²⁶ *Opinion 1/15*, para. 214. See Kuner 2018.

²⁷ *Opinion 1/15*, paras. 93, 134 and 214.

safeguards for the data subjects’. Requiring ‘appropriate safeguards for data subjects’ seems to be a weaker standard than that contained in Article 44 GDPR, which provides that any data transfers must comply with both the conditions laid down in Chapter V and with the other provisions of the GDPR, and it can be questioned whether this standard complies with the standard for adequacy set out by the CJEU.

The EDPB uses the term ‘international agreement’ to describe the ‘legally binding and enforceable instrument’ of Article 46(2)(a) and the ‘administrative arrangements’ of Article 46(3)(b) GDPR.²⁸ For the EDPB international agreements therefore qualify as appropriate safeguards as can also be seen in a statement issued in 2021, where it urges all Member States to review their existing agreements in light of its guidance.²⁹ This classification would seem to require international agreements to provide essential equivalence with EU law, despite the lower standard required by recital 102. In neither document does the EDPB expand on its reasoning for this classification nor on the question of whether all international agreements can thus be regarded as appropriate safeguards. The Commission has adopted the EDPB’s categorisation in its GDPR evaluation of 2024.³⁰

Article 96 provides that ‘international agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked’. However, it is questionable whether this is compatible with the dynamic approach to fundamental rights protection that the CJEU adopted in *Schrems I and II* (discussed below).³¹

An adequacy decision is adopted unilaterally by the Commission, which may also repeal, amend or suspend it.³² However, its adoption is preceded by extensive and lengthy negotiations with the third country or international organisation,³³ and may be supported by cooperation mechanisms agreed with them.³⁴ The term ‘international agreement’ is defined flexibly under EU law as an undertaking subject to international law that has binding force,³⁵ and adequacy decisions are gradually coming to resemble international agreements more than purely unilateral acts.

Whether the EU institutions decide to use an adequacy decision or an international agreement as a legal basis for data transfers depends on a variety of factors, both legal and political. An adequacy decision is based on a more thorough investigation of data protection standards in third countries than is usually possible when negotiating an international agreement. The Commission has determined that data transfers in the context of international trade are to be legalised by adequacy decisions rather than by international agreements, based on a desire to avoid political controversy.³⁶

²⁸ EDPB 2020B, p. 5 FN3.

²⁹ EDPB 2021A.

³⁰ EC Communication 2024, p. 24.

³¹ *Opinion 1/15*, paras. 93, 134 and 214.

³² Art. 45(5) GDPR.

³³ See, e.g., Drechsler 2022 regarding the negotiations for the Japanese adequacy decision.

³⁴ For example, the EU-US Privacy Framework is supported by enforcement cooperation between the US Federal Trade Commission and the EU supervisory authorities in the course of implementing the Decision. See Commission Decision EU-US Data Privacy Framework, at L 231/210.

³⁵ See Koutrakos 2018, p. 1142 (electronic edition).

³⁶ See EC Communication 2017, p. 9. See also Yakovleva and Irion, p. 218; Yakovleva 2024; Hanke 2017.

However, the legal relationship between international agreements and adequacy decisions remains confused, as illustrated by the so-called Umbrella Agreement between the EU and the US dealing with the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences.³⁷ While stating on the one hand that it does not provide a legal basis for data transfers under the LED,³⁸ the Umbrella Agreement also proclaims that data processing under it shall be deemed to comply with laws restricting the international transfer of data,³⁹ which makes it seem to resemble an adequacy decision. Potentially, the Umbrella Agreement has to be classified as an appropriate safeguard for the LED,⁴⁰ leaving the task of assessing the actual level of protection provided to the exporting law enforcement authorities.⁴¹ Several other treaties provide a legal basis for transfers of personal data to third countries; these are discussed in the commentary on Article 44 in this edition.

Adequacy decisions also have implications for the EEA and EFTA states. The EEA is comprised of the EU Member States plus Iceland, Liechtenstein and Norway, which three countries together plus Switzerland comprise the EFTA. The EEA Agreement, as amended in July 2018,⁴² incorporates the GDPR into its Annexes and provides that the provisions of the GDPR should be read, for the purposes of that Agreement, with a number of adaptations affecting the three EEA/EFTA States⁴³ and the EFTA Surveillance Authority. In this respect, the amended Agreement provides that additional provisions shall be inserted after Article 45(1) GDPR with regard to data transfers from the EEA/EFTA States.⁴⁴

3. National developments

Article 45 does not foresee implementation by the Member States. Legislation of some Member States provides for DPAs to suspend their proceedings and refer questions about adequacy decisions of the Commission for a court decision,⁴⁵ as provided for in CJEU's *Schrems I* judgment.⁴⁶

In its *Schrems II* judgment, the CJEU held that 'the validity of provisions of EU law and, in the absence of an express reference to the national law of the Member States, their interpretation, cannot be construed in the light of national law, even national law of constitutional status, in particular fundamental rights as formulated in the national constitutions'.⁴⁷ The fact that Article 45 GDPR does not grant any role to Member State law thus means that its provisions cannot be construed in light of national law. In particular, until a Commission adequacy decision is declared invalid by the CJEU, 'the Member States and their organs, which include their independent supervisory authorities, cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection...and, as a result, to suspend or prohibit transfers of

³⁷ Umbrella Agreement US.

³⁸ Ibid., Art. 1(3). See also EDPS 2016, p. 7, finding that the Umbrella Agreement is not itself an adequacy decision.

³⁹ Art. 5(3) Umbrella Agreement US.

⁴⁰ Art. 37(1)(a) LED.

⁴¹ EDPB 2024A, pp. 10-12.

⁴² EEA Decision 2018.

⁴³ Switzerland, the fourth EFTA State is not a signatory to the EEA.

⁴⁴ Art. 5e(m) EEA Decision 2018.

⁴⁵ See e.g. German GDPR Implementation Law, s. 21.

⁴⁶ Case C-362/14, *Schrems I*, para. 65.

⁴⁷ Case C-311/18, *Schrems II*, para. 100.

personal data to that third country’.⁴⁸ Nevertheless, some lower Member State courts have occasionally interpreted Chapter V in ways that seem to diverge from its interpretation by the CJEU and the EDPB.⁴⁹ The EDPB has also stated that the supplemental transfer tools required under Article 46⁵⁰ are not required for transfers made using an adequacy decision.⁵¹

4. Case law

The CJEU has opined on the level of protection for international data transfers under the DPD and GDPR in *Schrems I*, Opinion 1/15, and *Schrems II*, which are discussed at length here. The CJEU also dealt with the DPD’s provisions on international data transfers in *Lindqvist*,⁵² which is discussed in the commentary on Article 44 in this edition. Some decisions from courts besides the CJEU are also discussed below in section 4.4.

4.1 *Schrems I*

The complainant Maximilian Schrems brought several complaints against Facebook before the Irish Data Protection Commissioner (‘DPC’), based on, among other things, Facebook’s international personal data transfers under the EU-US Safe Harbour Agreement.⁵³ In 2013, Schrems sought judicial review in the Irish High Court against the DPC’s decision not to proceed against Facebook as it felt incompetent to assess the existing decision. On 18 June 2014, Mr Justice Hogan of the High Court referred two questions about the case to the CJEU.⁵⁴

In its judgment, the CJEU broadly agreed with the conclusions of Advocate General Bot,⁵⁵ finding that the DPAs were not prevented by Article 25(6) from examining claims related to the adequacy of protection under a Commission decision, and that the decision underlying the Safe Harbour was invalid. The CJEU found that all provisions of the DPD must be interpreted in light of a high level of fundamental rights protection under the Charter. In considering the powers of the DPAs, it stressed the importance of their independence, and mentioned that their powers do not extend to data processing carried out in a third country. It further held that the transfer of personal data to a third country is itself an act of data processing, and thus falls within Member State law transposing the DPD and the supervisory powers of the DPA. The Court went on to find that a Commission decision cannot preclude an individual from filing a claim with a DPA concerning the adequacy of protection, nor can such a decision eliminate or reduce their powers.

Thus, when an individual makes a claim to a DPA contesting the compatibility of a data transfer based on an adequacy decision, the DPA must examine the claim ‘with all due diligence’.⁵⁶ When the DPA rejects such a claim as unfounded, the individual must have access to judicial remedies allowing him to contest this decision before national courts, and such courts ‘must stay proceedings and make a reference to the Court for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, as the case

⁴⁸ Ibid., para. 118.

⁴⁹ Landesgericht Traunstein, final judgment of 8 July 2024. See further Christakis, Felz and Swire 2024.

⁵⁰ See the commentary on Art. 46 in this edition.

⁵¹ EDPB 2021C, p. 12.

⁵² Case C-101/01, *Lindqvist*.

⁵³ The following analysis is adapted from Kuner 2017.

⁵⁴ See the Irish High court in *Schrems* [2014]; and *Schrems* (No. 2) [2014].

⁵⁵ Case C-362/14, *Schrems I* (AG Opinion).

⁵⁶ Case C-362/14, *Schrems I*, para. 63.

may be, raised by them of their own motion are well founded'.⁵⁷ Conversely, when the DPA finds such claim to be well-founded, it must 'be able to engage in legal proceedings', and the national legislature must 'provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity'.⁵⁸

The CJEU went on to find that the term 'an adequate level of protection' as used in the DPD must be understood as 'requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter', while not requiring that the level be identical to that under EU law.⁵⁹ Without this requirement, 'the high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries'.⁶⁰ While the means to which a third country has recourse for ensuring a high level of protection may differ from those employed within the EU, they must prove to be effective in practice.

Assessing the level of protection in a third country requires the Commission to 'take account of all the circumstances surrounding a transfer of personal data to a third country',⁶¹ to check periodically whether the adequacy assessment is still justified and to take account of circumstances that have arisen after adoption of the decision. This means that 'the Commission's discretion as to the adequacy of the level of protection ensured by a third country is reduced, with the result that review of the requirements stemming from Article 25 of Directive 95/46, read in the light of the Charter, should be strict'.⁶²

The CJEU then dealt with the validity of the Safe Harbour adequacy decision. While it found that 'a system of self-certification is not in itself contrary to the requirement laid down in Article 25(6) of Directive 95/46 that the third country concerned must ensure an adequate level of protection "by reason of its domestic law or . . . international commitments"', the reliability of such a system is based on 'the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data, to be identified and punished in practice'.⁶³ It noted that public authorities in the US were not required to comply with the Safe Harbour principles, and that the Safe Harbour decision of the Commission did not contain sufficient findings explaining how the US ensures an adequate level of protection.

The CJEU stated that under the Safe Harbour decision, the applicability of the principles could be limited to meet, for example, national security, public interest or law enforcement requirements, and that the decision stated that '[c]learly, where US law imposes a conflicting

⁵⁷ Ibid., para. 64.

⁵⁸ Ibid., para. 65.

⁵⁹ Ibid., para. 73.

⁶⁰ Ibid.

⁶¹ Ibid., para. 75.

⁶² Ibid., para. 78.

⁶³ Ibid., para. 81.

obligation, US organisations whether in the Safe Harbor or not must comply with the law'.⁶⁴ It found that these provisions in effect gave US law primacy over EU fundamental rights in situations where they conflict, and that to establish an interference with fundamental rights, 'it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference'.⁶⁵ Moreover, the Safe Harbour decision did not contain any finding concerning limitations on the powers of public authorities (such as law enforcement authorities) in the US to interfere with fundamental rights. The CJEU stated that:

legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail.⁶⁶

It found that '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',⁶⁷ and that 'legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter'.⁶⁸

In the judgment, the CJEU gave the following points of orientation to interpret the concept of essential equivalence:

1. There must be a high level of fundamental rights protection, which must be evaluated strictly.
2. The third country in question must have a means for ensuring a high level of protection that is effective in practice, in light of all the circumstances surrounding a transfer of personal data to a third country. This must include periodic checks as to whether the adequacy assessment is still justified and take into account all circumstances that have arisen after adoption of the decision.
3. Adequate protection must take into account the country's domestic law or international commitments.
4. Any system of self-certification must be reliable based on effective detection and supervision mechanisms enabling infringements of the rules, in particular the right to respect for private life and the protection of personal data, to be identified and punished in practice.
5. An adequacy decision must include a detailed explanation of how a country ensures an adequate level of protection.
6. There must not be limitations based on national security, public interest or law enforcement requirements that give third country law primacy over EU law.

⁶⁴ Ibid., para. 85.

⁶⁵ Ibid., para. 87.

⁶⁶ Ibid., para. 93.

⁶⁷ Ibid., para. 94.

⁶⁸ Ibid., para. 95.

7. Limitations must be placed on the power of public authorities (such as law enforcement authorities) to interfere with fundamental rights. In particular, any such access must be strictly necessary and proportionate to the protection of values such as national security, there must be clear and precise rules regarding the scope of application of a measure, and for effective protection against the risk of abuse of data, and derogations and limitations in relation to data protection should apply only when strictly necessary.
8. Third country legislation must not authorise, on a generalised basis, storage of all the personal data transferred without any differentiation, limitation or exception being made in light of the objective pursued and without an objective criterion being laid down to determine the limits to the data, and its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference entailed by access to that data and its use.

The significance of *Schrems I* goes beyond its data protection implications. As President of the CJEU Koen Lenaerts has stated, the *Schrems I* judgment is ‘a landmark case’ in EU procedural law ‘because it has made clear that the preliminary reference for controlling the validity of an act of the Union is not only without limit in time . . . but also may be reviewed in terms of the legal framework existing at the date of the Court’s judgment’.⁶⁹ Thus, the Charter, under which the CJEU evaluated the Safe Harbour Framework in *Schrems I*, had not been elevated to the level of EU primary law at the time the Safe Harbour was enacted in 2000, but the Court still used it as the standard of reference. More specifically, the Court’s dynamic approach to fundamental rights protection in *Schrems I* can also be seen in its choice of ‘essential equivalence’ with EU law as the measure of ‘adequate protection’, even though when the DPD was adopted, the EU legislator specifically preferred the term ‘adequate protection’ over ‘equivalent protection’.⁷⁰ This indicates that in cases involving the validity of adequacy decisions (and possibly other data transfer mechanisms as well), the CJEU makes a ‘dynamic assessment’ and evaluates whether they meet the legal standards in force at the time that it makes its judgment and not just those that applied when the case was brought.⁷¹

4.2 Opinion 1/15

An agreement for the processing and transfer of PNR data between the EU and Canada was initialed by the EU Council of Ministers and Canada on 6 May 2013⁷² (referred to here as the Draft Agreement) and signed on 25 June 2014,⁷³ following which the Council sought approval of it by the European Parliament.⁷⁴ On 25 November 2014, the Parliament adopted a resolution seeking an opinion from the CJEU pursuant to Article 218(11) on two questions,⁷⁵ which application was lodged with the Court on 10 April 2015.⁷⁶ The two questions were as follows:

⁶⁹ Lenaerts speech 2018, between 27’07” and 30’35”.

⁷⁰ Simitis and Dammann 1997, p. 273. See also Yakovleva 2024, pp. 263-269.

⁷¹ See in this regard Case C-311/18, *Schrems II*, para. 71, where the CJEU refused to find the case inadmissible on the grounds that it was based on the DPD which has been repealed by the GDPR, stating that ‘it must be borne in mind that the Court has a duty to interpret all provisions of EU law which national courts require in order to decide the actions pending before them, even if those provisions are not expressly indicated in the questions referred to the Court of Justice by those courts... On those grounds, the fact that the referring court referred its questions by reference solely to the provisions of Directive 95/46 cannot render the present request for a preliminary ruling inadmissible’.

⁷² Proposal PNR Canada 2013.

⁷³ Press Release PNR Canada 2014.

⁷⁴ The following analysis is adapted from Kuner 2018.

⁷⁵ EP Resolution 2014.

⁷⁶ EP Request Opinion 1/15.

Is the envisaged agreement compatible with the provisions of the Treaties (Article 16 TFEU) and the Charter of Fundamental Rights of the European Union (Articles 7, 8 and Article 52(1)) as regards the right of individuals to protection of personal data?

Do Articles 82(1)(d) and 87(2)(a) TFEU constitute the appropriate legal basis for the act of the Council concluding the envisaged agreement or must that act be based on Article 16 TFEU?

In his Opinion issued on 8 September 2016,⁷⁷ Advocate General Mengozzi responded negatively to both questions, as he found several provisions of the Draft Agreement incompatible with the Charter. He also found that the correct legal basis of the Agreement was provided by Articles 16(2) (the right to data protection) and 87(2)(a) Treaty on the Function of the European Union ('TFEU') (police cooperation among the Member States in criminal matters) and not by Article 82(1)(d) TFEU (judicial cooperation in criminal matters in the Union).

In its Opinion of July 2017,⁷⁸ the Court first noted that an international agreement must be entirely compatible with the treaties and constitutional principles of the EU.⁷⁹ The CJEU found that the Draft Agreement had the dual objectives of protecting public security and data protection, both of which are inextricably linked.⁸⁰ Thus, the Court agreed with the above conclusions of the Advocate General concerning the legal basis.

The Court found that PNR data may reveal considerable detail about an individual, such as their travel habits, relationships and financial situation, which may also include sensitive information. It stressed that the data were to be systematically analysed by automated means before arrival in Canada, and that they could be stored for up to five years. Thus, the Court observed that the transfer of PNR data to Canada and the rules foreseen in the Draft Agreement would entail an interference with the fundamental rights to respect for private life under Article 7⁸¹ and to the protection of personal data under Article 8 of the Charter.⁸²

Since Article 7 and Article 8 are not absolute rights,⁸³ the Court then examined whether such interferences could be justified. It found that the processing of PNR data under the Draft Agreement pursued a different objective from that for which it was collected by air carriers, and thus required a different legal basis, such as separate consent by passengers or some other legal basis laid down by law.⁸⁴ The Court next found that an international agreement may meet the requirements of being a 'law' as defined in Articles 8(2) and 52(1) of the Charter.⁸⁵ It went on to note that in this case such interferences are justified by the need to fight terrorism and serious transnational crime in order to ensure public security, and that the transfer of PNR data to Canada and its subsequent processing may be appropriate to meet that objective.⁸⁶

⁷⁷ *Opinion 1/15* (AG Opinion).

⁷⁸ *Opinion 1/15*.

⁷⁹ *Ibid.*, para. 67.

⁸⁰ *Ibid.*, para. 94.

⁸¹ *Ibid.*, para. 125.

⁸² *Ibid.*, para. 126.

⁸³ *Ibid.*, para. 136.

⁸⁴ *Ibid.*, para. 143.

⁸⁵ *Ibid.*, paras. 145–147.

⁸⁶ *Ibid.*, paras. 151 and 153.

The CJEU then analysed the protections provided in the Draft Agreement, and had the following criticisms:

1. The Draft Agreement was not sufficiently precise in specifying the PNR data to be transferred.
2. It did not provide sufficient protections for the transfer of sensitive data. In addition, it stated that ‘a transfer of sensitive data . . . requires a particularly solid justification, based on grounds other than the protection of public security against terrorism and serious transnational crime’.⁸⁷
3. With regard to automated analyses of PNR data, because of the margin of error, any positive result had to be subject to ‘individual re-examination by non-automated means’ before any measure adversely affecting a passenger was taken.⁸⁸
4. Language permitting Canada to process PNR data on a case-by-case basis to ‘ensure the oversight or accountability of the public administration’ and to ‘comply with the subpoena or warrant issues, or an order made, by a court’ lacked sufficient clarity and precision.⁸⁹

The Court also noted that the coverage of all air passengers flying between the EU and Canada was not unacceptably broad, particularly since Article 13 of Convention on Civil Aviation (the Chicago Convention)⁹⁰ require signatories (which include Canada and all EU Member States, but not the EU itself) to comply with admission and departure formalities of passengers from their territory, which can include security checks laid down by Canadian law.⁹¹

The Court then discussed at length the compatibility of the Draft Agreement with EU law requirements for data retention. With regard to the retention and use of PNR data before the arrival of passengers, during their stay in Canada, and on their departure, the Court found that some elements of the retention of data under the Draft Agreement were acceptable, such as the use of data for security checks and border control checks;⁹² verifying the reliability and topicality of models for the automated processing of data;⁹³ or cases when data are collected by the Canadian authorities during the individuals’ stay in Canada indicating that use of it may be necessary to combat terrorism and serious transnational crime.⁹⁴ However, the Court stated that the use of PNR data should be subject to prior review by a court or an administrative body, and that otherwise it may be found to go beyond what is strictly necessary.⁹⁵

With regard to the retention and use of PNR data after passengers’ departure from Canada, the Court found that this was not strictly necessary,⁹⁶ but that it could be stored in Canada in cases where certain passengers may present a risk of terrorism or serious transnational crime. It stated that the five-year retention period in the Draft Agreement does not exceed the limits of what is

⁸⁷ Ibid., para. 165.

⁸⁸ Ibid., para. 173.

⁸⁹ Ibid., para. 181.

⁹⁰ Aviation Convention 1944.

⁹¹ *Opinion 1/15*, paras. 188–189.

⁹² Ibid., para. 197.

⁹³ Ibid., para. 198.

⁹⁴ Ibid., para. 199.

⁹⁵ Ibid., paras. 201–203.

⁹⁶ Ibid., paras. 206 and 211.

strictly necessary,⁹⁷ but that use of such data should be subject to prior review by a court or ‘independent administrative body’.⁹⁸

Concerning the disclosure of PNR data to government authorities, the Court reiterated the standard it set forth in *Schrems I* that data transfers to third countries require a level of protection that is ‘essentially equivalent’ to that under EU law,⁹⁹ and held that this also applies to PNR transfers to Canada. The Court went on to say that this required either an international agreement between the EU and a third country, or an adequacy decision of the Commission.¹⁰⁰ It held that individuals must have a right to have their data rectified,¹⁰¹ and that they must be notified individually when their data are used by a judicial authority or independent administrative body¹⁰² unless this would jeopardise an investigation.¹⁰³ Finally, the Court held that the Draft Agreement did not sufficiently guarantee that oversight of compliance with its rules would be carried out by an independent authority within the meaning of Article 8(3) of the Charter.¹⁰⁴ Thus, the Court found that the Draft Agreement could not be concluded in its current form.

4.3 *Schrems II*

In its *Schrems II* judgment, the CJEU invalidated the Commission decision underlying the EU-US Privacy Shield, the successor of the Safe Harbour Agreement. The judgment can be seen as a continuation and strengthening of the standards the Court articulated in *Schrems I* and *Opinion 1/15*.

After the CJEU invalidated the Safe Harbour adequacy decision in its *Schrems I* decision of 6 October 2015, the Irish High Court annulled the decision rejecting Schrems’ complaint and referred the case back to the DPC. After investigating Schrems’ allegations, the DPC brought proceedings before the High Court, which concerned, among other things, US law and practice regarding surveillance and the level of protection provided by the EU-US Privacy Shield. On 9 May 2018, the High Court stayed the proceedings and referred eleven questions to the CJEU, several of which concerned the validity of the Privacy Shield.

In his Opinion, Advocate General Saugmandsgaard Øe found that there was no need to examine the validity of the Privacy Shield,¹⁰⁵ but also criticised it strongly.¹⁰⁶ The Court’s subsequent decision to invalidate the Privacy Shield was based on four factors: (1) the primacy of US law enforcement requirements over those of the Privacy Shield;¹⁰⁷ (2) a lack of necessary limitations and safeguards on the power of the authorities under US law, particularly in light of proportionality requirements;¹⁰⁸ (3) the lack of an effective remedy in the US by EU data subjects;¹⁰⁹ and (4) deficiencies in the Privacy Shield Ombudsman mechanism.¹¹⁰ In its

⁹⁷ Ibid., para. 209.

⁹⁸ Ibid., para. 208.

⁹⁹ Ibid., paras. 134 and 214.

¹⁰⁰ Ibid., para. 214.

¹⁰¹ Ibid., para. 220.

¹⁰² Ibid., para. 223.

¹⁰³ Ibid., para. 224.

¹⁰⁴ Ibid., para. 231.

¹⁰⁵ Case C-311/18, *Schrems II* (AG Opinion), paras. 161ff.

¹⁰⁶ Ibid., paras. 196ff.

¹⁰⁷ Case C-311/18, *Schrems II*, para. 164.

¹⁰⁸ Ibid., paras. 168-185.

¹⁰⁹ Ibid., paras. 191-192.

¹¹⁰ Ibid., paras. 193-197.

evaluation of these issues, the Court paid particular concern to Articles 7, 8, and 47 of the Charter. In light of these deficiencies, the Court found that the Privacy Shield Decision was invalid¹¹¹ with immediate effect.¹¹²

The judgment is important for adequacy decisions in two respects. First of all, it reinforces the conclusions reached by the Court in *Schrems I* with regard to the high standard of protection necessary for an adequacy decision, and the fact that such standard must be based on the Charter. In *Schrems II*, the Irish High Court heard extensive testimony by experts concerning privacy and intelligence-gathering in the US,¹¹³ so that the decision of the CJEU is based on a record that provided the opportunity for a considered evaluation of US law and practice. This solidifies the high standard that the Court requires for data transfers to third countries in general, and to the US in particular. Second, the Court's application of the Article 45 standard of essential equivalence to other data transfer mechanisms as well¹¹⁴ indicates that the Court views this standard as underlying the rationale of Chapter V GDPR to avoid the circumvention of EU law,¹¹⁵ and that it is likely to apply it to other data transfer situations in the future as well.

Schrems II also has important implications for the use of appropriate safeguards to transfer personal data, which are discussed in the commentary on Article 46 in this edition.

4.4 Other jurisdictions

In deciding important cases dealing with the adequacy of protection for international data transfers, other courts have indicated that standards for the adequate protection of data transfers may differ between EU law and other European legal systems. In *Big Brother Watch and Others v United Kingdom*, the Grand Chamber of the European Court of Human Rights (ECtHR) stated that government transfers of data to other countries or international organisations acquired through secret measures of telecommunications surveillance must be subject to certain protections, but that 'this does not necessarily mean that the receiving State must have comparable protection to that of the transferring State...'.¹¹⁶ An almost identical phrasing was used in the *Centrum för Rättvisa v Sweden* judgment issued on the same day also by the Grand Chamber of the ECtHR.¹¹⁷ Both judgments confirm that for transfers between intelligence agencies, the ECtHR applies a different standard than the one recognised by the CJEU. As the partly concurring and partly dissenting opinion of judge Pinto De Albuquerque in *Big Brother Watch and Others v United Kingdom* puts it, 'the Strasbourg Court lags behind the Luxembourg Court, which remains the lighthouse for privacy rights in Europe'.¹¹⁸

Both judgments further clarify the contours of an effective remedy for cases of governmental access involving intelligence agencies — a key concern also for the CJEU as described earlier. Both judgments highlight that the effective remedy of an individual needs to lead to a reasoned

¹¹¹ Ibid., para. 201.

¹¹² Ibid., para. 202.

¹¹³ See Case C-311/18, *Schrems II* (AG Opinion), para. 53.

¹¹⁴ Case C-311/18, *Schrems II*, paras. 92 and 105.

¹¹⁵ See Case C-362/14, *Schrems I*, para. 73.

¹¹⁶ ECtHR, *Big Brother Watch and Others* (Grand Chamber), para. 362. See also the commentary on Art. 44 in this edition.

¹¹⁷ ECtHR, *Centrum för Rättvisa v Sweden* (Grand Chamber), para. 276.

¹¹⁸ ECtHR, *Big Brother Watch and Others* (Grand Chamber), Partly Concurring and Partly Dissenting Opinion of Judge Pinto Albuquerque, para. 59.

and legally binding decision on the lawfulness of the access.¹¹⁹ In *Centrum för Rättvisa v Sweden*, the absence of such reasoning was found to be a severe shortcoming of the Swedish system contributing to the finding of a violation of Article 8 ECHR by the ECtHR.¹²⁰ Yet, in a recent admissibility decision, the ECtHR suggests that such reasoning might not always have to be available.¹²¹

The topic of potentially different standards is not exclusive to the relationship between the CJEU and the ECtHR. A judgment of the German Federal Constitutional Court (*Bundesverfassungsgericht*) also indicates that there are different standards for data transfers under German constitutional law than under EU law and the Charter.¹²²

The national level has also seen a number of important decisions by DPAs regarding transfers based on adequacy decisions, especially in the aftermath of the *Schrems II* judgment. Two examples are illustrative for the ongoing discussions. First, the DPC issued a record fine of EUR 1.2 billion against Meta (formerly Facebook) together with a suspension order for the transfers in question for its lack of a legal basis to transfer personal data to the US, once the Privacy Shield was invalidated with immediate effect as a continuation of the *Schrems* saga in Ireland.¹²³ The main argument of the DPC was that the SCCs used by Meta after the end of the Safe Harbour Agreement were not accompanied by the required supplementary measures to ensure an equivalent level of protection given the conclusions the CJEU reached on the level of protection in the US when invalidating the Privacy Shield.¹²⁴ The fine and suspension order were a direct result of a binding decision of the EDPB issued via the GDPR's dispute resolution mechanism, as the DPC had originally decided not to impose a fine.¹²⁵ Meta has since challenged the EDPB's binding decision before the General Court.¹²⁶

Second, in another case dealing with the interim period between the annulation of the Privacy Shield and the new adequacy mechanism for the US (the Data Privacy Framework), the Dutch data protection authority fined Uber EUR 290 million for the lack of a legal basis justifying the transfer to the US.¹²⁷ Uber had in the aftermath of *Schrems II* eventually cancelled its SCCs without replacing them with another appropriate safeguard of Article 46, leading to a period with no transfer mechanism in place.¹²⁸ Further examples can be found in the outcomes of the 101 complaints before DPAs brought by the NGO noyb in the aftermath of *Schrems II*. These complaints were brought against websites using 'Google Analytics' or 'Facebook Business Tools', as both involved a transfer to the US, which after the annulation of the Privacy Shield may often lack a legal basis.¹²⁹ The complaints eventually led to the creation of an EDPB taskforce and several national DPA decisions discussing the role of risk in the assessment of essential equivalence,¹³⁰ which topic is explored further in the commentary on Article 46 of this edition. Enforcement action concerning data transfers has also occurred under the EUDPR.

¹¹⁹ ECtHR, *Big Brother Watch and Others (Grand Chamber)*, para. 359; ECtHR, *Centrum för Rättvisa v Sweden* (Grand Chamber), para. 362.

¹²⁰ ECtHR, *Centrum för Rättvisa v Sweden* (Grand Chamber), para. 362.

¹²¹ ECtHR, *Association Confraternelle de la presse judiciaire et autres*, para. 119.

¹²² Bundesverfassungsgericht, judgment 1 BvR 966/09 of 20 April 2016, para. 335. See also the commentary on Art. 44 in this edition.

¹²³ DPC 2023, para. 10.5 and 10.11.

¹²⁴ Ibid., section 7.

¹²⁵ EDPB 2023C, paras. 270-279.

¹²⁶ Case T-325/23, *Meta Platforms Ireland v EDPB*.

¹²⁷ Dutch DPA 2024, paras. 137-166.

¹²⁸ Ibid., paras. 105-111.

¹²⁹ See for an overview of decisions in that context Noyb Website Data Transfers.

¹³⁰ EDPB 2023B.

In one decision, the EDPS found that the European Commission's use of Microsoft 365 infringed the data transfer provisions of the EUDPR, in particular concerning transfers to the US before and after invalidation of the Privacy Shield following *Schrems II*.¹³¹

C. Analysis

1. Procedure for adequacy decisions

Article 45 deals with the issuance of formal decisions concerning adequacy by the Commission. Such decisions are implementing acts issued based on the examination procedure set out in Article 5 of the so-called Comitology Regulation.¹³² The adoption of implementing acts is covered in detail in the commentary on Article 93 GDPR in this edition. An implementing act declaring that adequate protection is ensured is set out in a Commission decision.¹³³ The procedure gives considerable power to the Commission, as it is the institution which proposes and enacts adequacy decisions, and the opinions and resolutions of the European Parliament and the EDPB regarding them are not binding on it.¹³⁴ The Commission has no official milestones to meet or strict deadlines for its assessment either, further cementing its role as an assessor and arbiter of adequacy.¹³⁵

The issuance and negotiation of an adequacy decision typically begins with a third country approaching the Commission and requesting that discussions be opened. Negotiations between the Commission and a third country concerning adequacy generally take several years, and can become entangled in political factors that can lead to tensions.¹³⁶ In the course of the procedure, the Commission has typically made its own investigations about the adequacy of protection in third countries, including through reports by academic experts.¹³⁷ Documents concerning the Commission's deliberations, including such academic studies, have typically not been made public, and stakeholders have criticized a lack of transparency concerning the entire procedure.¹³⁸ Typically few changes are made to a draft decision once it is issued, due to the international negotiations preceding it. However, it can be hoped that international cooperation may gradually strengthen the basis for protection under adequacy decisions.¹³⁹

¹³¹ EDPS 2024.

¹³² Regulation 182/2011. See Art. 93(2) GDPR.

¹³³ All Commission adequacy findings are entitled 'decisions', except for one, the UK decision concerning data transfers under the GDPR, which is entitled 'Commission Implementing Regulation' (Commission Decision UK GDPR). The reason for this difference in nomenclature is unclear, but it does not seem to have any legal significance.

¹³⁴ Czerniawski 2024.

¹³⁵ Ibid., pp. 218-220.

¹³⁶ For example, in July 2010 the government of Ireland delayed an EU adequacy decision for Israel based on alleged Israeli government involvement in the forging of Irish passports (see Ihle 2010). Israel later received an adequacy decision from the European Commission. See also Stoddart, Chan and Joly 2016 concerning tensions with Quebec concerning adequacy.

¹³⁷ See e.g. Commission Staff Working Document 2006, p. 3, referring to such an academic study.

¹³⁸ See e.g. Council Position on GDPR Evaluation 2023; Multistakeholder Expert Group Report 2024, pp. 18-19. Complaints about the lack of transparency extend further to the EDPB, which in 2023 was reprimanded by the European Ombudsman about its lack of transparency for documents surrounding its work on international personal data transfers. See European Ombudsman 2023.

¹³⁹ See, e.g., Commission Decision EU-US Data Privacy Framework 2023, at L 231/210, discussing enforcement cooperation between the US Federal Trade Commission and the EU DPAs in the course of implementing the Decision. See also the commentary on Art. 50 in this edition.

It is unclear how the Commission decides on the next candidate for an adequacy decision.¹⁴⁰ In 2018, the Commission stated the following concerning its strategy:

Under its framework on adequacy findings, the Commission considers that the following criteria should be taken into account when assessing with which third countries a dialogue on adequacy should be pursued:

- (i) the extent of the EU's (actual or potential) commercial relations with a given third country, including the existence of a free trade agreement or ongoing negotiations;
- (ii) the extent of personal data flows from the EU, reflecting geographical and/or cultural ties;
- (iii) the pioneering role the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region; and
- (iv) the overall political relationship with the third country in question, in particular with respect to the promotion of common values and shared objectives at international level.¹⁴¹

These criteria reveal a purposefully linking of political considerations such as trade relationships with the adequacy process,¹⁴² illustrating the increasingly political nature of such decisions.

Decisions by the Commission concerning adequacy, or decisions finding that an adequate level of protection is or is no longer ensured, must be published in the Official Journal of the EU.¹⁴³ Before reaching a decision on adequacy, the Commission must consult the EDPB. The EDPB is to be provided by the Commission with all relevant documentation, including correspondence, findings and the Commission's report on the level of protection in the third country or international organisation.¹⁴⁴ The EDPB will then issue its own opinion on the Commission's findings.¹⁴⁵ The fact that the GDPR does not mention a power by the EDPB to approve the Commission's decision¹⁴⁶ confirms that its opinion is not binding.¹⁴⁷ The European Parliament also usually adopts a resolution on a proposed Commission adequacy decision, although such vote is not binding on the Commission.¹⁴⁸

In adopting adequacy decisions, the Commission is assisted by a committee of Member State representatives¹⁴⁹ (the successor to the 'Article 31 Committee' under the DPD) that must

¹⁴⁰ Czerniawski 2024, p. 229.

¹⁴¹ EC Communication 2018, p. 8.

¹⁴² On privacy and trade, see further Chander and Schwartz 2023; Yakovleva 2024.

¹⁴³ Art. 45(8) GDPR.

¹⁴⁴ WP29 2018, p. 4.

¹⁴⁵ Ibid.

¹⁴⁶ See Art. 70(1)(s), stating that the EDPB is to 'provide the Commission with an opinion' concerning adequacy, and rec. 105, stating that the Commission 'should consult' the EDPB.

¹⁴⁷ Thus, the Commission approved an adequacy decision covering the Japanese Act on the Protection of Personal Information in 2019 despite the fact that the opinion of the EDPB on the decision (EDPB 2018) criticised it. The same happened in the context of the adequacy decisions for the UK and the US. See EDPB 2021B; EDPB 2023A. The most positive assessment of the EDPB to date concerns the adequacy decision of the Republic of Korea. See EDPB 2021D.

¹⁴⁸ See, e.g., EP Resolution 2000, in which the Parliament voted against the proposed Commission decision on the EU-US Safe Harbor framework that was later adopted by the Commission, only to be invalidated in 2015 by the CJEU. The European Parliament issued similar resolutions against both the Privacy Shield and the Data Privacy Framework. See EP Resolution 2018; EP Resolution 2023.

¹⁴⁹ Art. 93(2) GDPR.

approve decisions in line with the examination procedure provided for by Article 5 of the Comitology Regulation, although its choice is limited to accepting or declining the draft decision (i.e., it cannot propose amendments).¹⁵⁰ The Commission plays a dominant role in the work of the committee, including convening and chairing the meetings, preparing the agenda, and deciding on the final wording of documents put to vote, which has led to criticism of the committee's oversight of the Commission.¹⁵¹

An adequacy decision must contain at least the following:

1. It must state specifically that the third country or international organisation ensures adequate protection by virtue of its domestic law or international commitments (this follows from para. 97 of the *Schrems I* judgment).
2. It must give the territorial and sectoral application of the decision (GDPR Article 45(3)).
3. It must provide for a mechanism for periodic review of the decision (Article 45(3)).
4. It must identify the supervisory authority or authorities with responsibility for ensuring and enforcing compliance with the data protection rules (Article 45(2)(b) and (3)).

In addition, the adequacy decision must not limit the power of the DPAs to investigate complaints about whether the level of protection set forth in a Commission adequacy decision is compatible with fundamental rights.¹⁵² Transfers under adequacy decisions do not require any further authorisation by DPAs or other authorities.¹⁵³

2. Scope of adequacy decisions

Adequacy decisions can be issued for any country that is not an EU Member State or party to the EEA. This means that no adequacy decision is needed with regard to data transfers to the three EEA countries. Commission adequacy decisions apply in the EEA countries once they are adopted into the list of EEA Joint Committee Decisions,¹⁵⁴ which has been done with all of the existing decisions.¹⁵⁵ Thus, they also apply for data transfers from Iceland, Liechtenstein and Norway as well. The GDPR was marked as EEA relevant and has been incorporated into the EEA Agreement.¹⁵⁶

Article 45 allows Commission decisions to be issued concerning not only third countries, but also 'a territory or one or more specified sectors within that third country' or, unlike the DPD, an international organisation. The reference to territories includes, for example, Overseas Countries and Territories ('OCTs') that have special links with either Denmark, France, or the Netherlands,¹⁵⁷ and those to which EU law does not apply under the TFEU.¹⁵⁸ All such

¹⁵⁰ Czerniawski 2024, p. 228.

¹⁵¹ Ibid., p. 236.

¹⁵² See Case C-362/14, *Schrems I*, para. 102.

¹⁵³ Art. 45(1) GDPR. See also Case C-311/18, *Schrems I*, para. 116.

¹⁵⁴ See EFTA 2017.

¹⁵⁵ See EEA Agreement, Annex XI, pp. 13–16. The latest decision 'the EU-US Data Privacy Framework' was added in September 2023. See *ibid.*, point 5ex.

¹⁵⁶ EEA Decision 2018.

¹⁵⁷ Under Annex II TFEU, OCTs include Greenland, New Caledonia and Dependencies, French Polynesia, French Southern and Antarctic Territories, Wallis and Futuna Islands, Mayotte, Saint Pierre and Miquelon, Aruba, Netherlands Antilles (Bonaire, Curaçao, Saba, Sint Eustatius and Sint Maarten), Anguilla, Cayman Islands, Falkland Islands, South Georgia and the South Sandwich Islands, Montserrat, Pitcairn, Saint Helena and Dependencies, British Antarctic Territory, British Indian Ocean Territory and Turks.

¹⁵⁸ Art. 355 TFEU. See also the commentary on Art. 3 in this edition.

territories can thus be the subject of an adequacy decision. However, EU law applies in Guadeloupe, French Guiana, Martinique, Réunion, Saint-Barthélemy, Saint-Martin, the Azores, Madeira and the Canary Islands,¹⁵⁹ so personal data can be transferred to them without an adequacy decision.

The possibility of adopting an adequacy decision for a ‘territory’ could in theory include one covering a state in a federal system (e.g., a US federal state such as California), though there may be political and legal issues with regard to the negotiation and implementation of such a decision. For example, the federal state would have to be able to commit in a legally binding fashion to abide by the conditions for adequacy set forth in Article 45 GDPR, which may present problems in light of its own constitutional status.

Several adequacy decisions cover a specific legal framework in a third country. The Canadian decision covers transfers to organisations subject to the Canadian Personal Information Protection and Electronic Documents Act;¹⁶⁰ the decision for Japan is limited to data importers that fall under the Japanese Act on the Protection of Personal Information, and does not cover some types of recipients such as the media, political parties, and academic institutions;¹⁶¹ and the US decision covers organisations that have joined the EU-US Data Privacy Framework.¹⁶² Further restrictions exist for example in the scope of the adequacy decision for the United Kingdom, the Republic of Korea, and the Faroe Islands.¹⁶³ It is the responsibility of the data exporter to verify whether the adequacy decision they intend to use as the legal basis for a transfer covers the processing operation in question.¹⁶⁴

The Commission has mentioned ‘financial services or IT sectors’ as potential subjects of adequacy decisions,¹⁶⁵ and has indicated that sectoral decisions ‘will need to be considered in light of elements such as, for instance, the nature and state of development of the privacy regime (stand-alone law, multiple or sectorial laws etc.), the constitutional structure of the third country or whether certain sectors of the economy are particularly exposed to data flows from the EU’.¹⁶⁶ The EDPB expects the Commission to clearly indicate it when an adequacy decision has partial or sectoral scope.¹⁶⁷

Article 45(1) also allows the Commission to issue adequacy decisions covering data transfers to international organisations. The concept of international organisation is defined under Article 4(26),¹⁶⁸ and data transfers to international organisations are also discussed in the Commentaries on Article 3 and Article 44. A number of complex issues under Article 45(2) would have to be clarified for an adequacy decision to be suitable for an international organization and acceptable to it, such as whether an international organisation is subject to national law; whether it is subject to independent supervision; and the extent of its participation in data protection obligations arising from legally binding conventions or multilateral or

¹⁵⁹ Art. 355(1) TFEU.

¹⁶⁰ Commission Decision Canada 2006, Art. 1.

¹⁶¹ Commission Decision Japan 2019, Arts. 1-2.

¹⁶² Commission Decision EU-US Data Privacy Framework, Art. 1.

¹⁶³ Commission Decision Faroe Islands 2010, Art. 2; Commission Decision UK GDPR 2021, Art. 1; Commission Decision Korea 2021, Art. 1.

¹⁶⁴ EDPB 2021C, pp. 9-10.

¹⁶⁵ EC Communication 2017, p. 8.

¹⁶⁶ Ibid.

¹⁶⁷ See, e.g., EDPB 2018, p. 11.

¹⁶⁸ See the commentary on Art. 4(26) in this edition.

regional systems.¹⁶⁹ Thus far there has been no adequacy decision covering an international organisation.

The level of protection granted by an adequacy decision must apply throughout the continuity of the transfer, i.e., it applies not only when the data have reached the country of data import but also when the data are in transit, such as when they are in the course of being transmitted to the destination via underseas cables. This position was affirmed by Advocate General Saugmandsgaard Øe in his Opinion in *Schrems II*,¹⁷⁰ although the Court did not mention this point in its judgment. Furthermore, the protection must continue when personal data are further shared in the country of data import.

On 31 January 2020, the UK left the European Union pursuant to the withdrawal procedure under Article 50 of the Treaty on European Union ('Brexit'). Thus, the UK is regarded as a third country for the purposes of international data transfers under Chapter V GDPR. The relationship between the EU and the UK is now governed by the Trade and Cooperation Agreement ('TCA') concluded between them.¹⁷¹ The Commission has issued two adequacy decisions covering data transfers to the UK under the GDPR and the LED respectively.¹⁷²

3. Criteria for adequacy

The GDPR does not contain a fixed definition of what an 'adequate level of protection' means, but refers to it in relation to certain criteria set out both in Article 45 and by the CJEU.¹⁷³ The approach to assessing adequacy has traditionally been based on determining whether law and practice in third countries results in the implementation of certain core EU data protection practices and principles.¹⁷⁴ These principles were originally set out by the WP29 in 1998 with an update in 2018 as including the purpose limitation principle; the data quality and proportionality principle; the transparency principle; the security principle; the rights of access, rectification and opposition; and restrictions on onward transfers.¹⁷⁵ In addition, the WP29 found that adequacy required the realisation of the basic objectives of a data protection system, namely delivering a good level of compliance with the rules; providing support and help to individual data subjects; and providing appropriate redress to the injured party when the rules are not complied with.¹⁷⁶

The criteria for adequacy in the GDPR have been significantly influenced by the CJEU's judgment in *Schrems I*, as discussed above. Article 45(2) contains a list of criteria that the Commission shall use when assessing the adequacy of protection which are much more detailed and extensive than those contained in Article 25(2) DPD and are partially derived from that judgment. Essential equivalence requires that a legal system fulfils the basic requirements of the rule of law, in particular free and fair elections; a separation of powers between the various branches of government; and an independent and impartial judiciary. Deviations from these factors will have a corresponding effect on any finding of adequacy.

¹⁶⁹ See Marelli 2021, pp. 24-25; Ntouvras 2019, pp. 275-76. See also Kuner 2019.

¹⁷⁰ Case C-311/18, *Schrems II* (AG Opinion), paras. 231-238.

¹⁷¹ Trade and Cooperation Agreement UK 2020.

¹⁷² See Commission Decision UK GDPR 2021 and Commission Decision UK LED 2021.

¹⁷³ See Schantz 2023, pp. 790-794 (Kindle edition).

¹⁷⁴ See WP29 1998; WP29 1997; WP29 2018.

¹⁷⁵ WP29 1998, p. 6; WP29 2018, pp. 5-6.

¹⁷⁶ WP29 1998, p. 7; WP29 2018, pp. 7-8.

Article 45(2)(c) states that a decision concerning adequacy should take into account ‘the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data’. This does not allow adequacy to be based solely on application of such an international convention or instrument, but indicates that it should be considered when assessing adequacy. In particular, a third country’s membership in the Council of Europe Convention 108 or Convention 108+ should be taken into account.¹⁷⁷ However, being bound by these international commitments does not automatically lead to a positive adequacy decision, as the WP29 found when it stated that membership in Convention 108 does not automatically lead to adequate protection for the purposes of the DPD.¹⁷⁸ The list of criteria to be taken into account when determining adequacy is not exhaustive, as shown by the fact that Article 45(2) states that the elements shall ‘in particular’ be taken into account. Accountability is also an important element of adequacy.¹⁷⁹

In its update of the adequacy criteria of 2018, — the paper has since been endorsed by the EDPB¹⁸⁰ — the WP29 found that a number of content and procedural or enforcement principles and mechanisms should exist in the data protection system of a third country or international organisation in order for it to be considered adequate.¹⁸¹ The following are the content principles that the WP29 enumerated:

1. Basic data protection concepts or principles (e.g. personal data, data controller, sensitive data, etc.).
2. Grounds for lawful and fair processing for legitimate purposes.
3. The purpose limitation principle.
4. The data quality and proportionality principle.
5. The data retention principle.
6. The security and confidentiality principle.
7. The transparency principle.
8. The right of access, rectification, erasure and objection.
9. Restrictions on onward transfers.

In addition, the WP29 required that additional content principles be applied when specific types of data processing are involved, in particular the processing of sensitive data, direct marketing and automated decision-making and profiling.¹⁸² The WP29 indicated that the non-existence of the rights to data portability or the restriction of processing in the third country’s or international organisation’s system should not be an obstacle for it to be recognised as essentially equivalent,¹⁸³ although it did not explain why it singled out those two rights. The WP29 neither supported nor excluded the possibility of an adequacy decision being issued if one of these content principles is excluded from its scope, e.g. whether an adequacy decision could be issued with regard to a third country whose data protection system did not provide special protections for sensitive data if the scope of the decision excluded the transfer of sensitive data.

¹⁷⁷ Rec. 105 GDPR.

¹⁷⁸ WP29 1998, pp. 8-9.

¹⁷⁹ See Docksey and Propp 2023.

¹⁸⁰ EDPB Endorsement.

¹⁸¹ WP29 2018, pp. 5-7.

¹⁸² *Ibid.*, p. 7.

¹⁸³ *Ibid.*, p. 6.

The WP29 also enumerated the following procedural and enforcement mechanisms that the data protection system of a third country or international organisation must contain:¹⁸⁴

1. A competent independent supervisory authority.
2. The data protection system must ensure a good level of compliance.
3. Accountability (i.e. obliging data controllers and/or those processing personal data on their behalf to comply with it and to be able to demonstrate such compliance in particular to the competent supervisory authority).
4. Providing support and help to data subjects in the exercise of their rights and appropriate redress mechanisms.

Finally, the WP29 also required, in line with Article 45(2)(a) GDPR, that third countries provide essential guarantees for law enforcement and national security access to limit interference with fundamental rights.¹⁸⁵ This means, in particular, the following:

1. Data processing should be based on clear, precise and accessible rules.
2. Necessity and proportionality must be demonstrated with regards to the legitimate objectives pursued.
3. The processing must be subject to independent oversight.
4. Effective remedies must be available to individuals.

These four requirements were further developed by the EDPB in the aftermath of *Schrems II* into the ‘essential guarantees’ that need to accompany governmental access in a data transfer context.¹⁸⁶

Governmental access has become an important issue in all adequacy decisions as well as in international discussions on international data flows.¹⁸⁷ In 2022, the OECD adopted a non-binding declaration on governmental access summarizing seven ‘shared’ principles that should govern governmental access to personal data held by private-sector organisations (legal basis, legitimate aims, approvals, data handling, transparency, oversight and redress).¹⁸⁸ The initiative has to be viewed as part of a broader push to create a ‘Data-Free-Flow-with-Trust’ system in the context of the World Economic Forum, originally proposed by Japan;¹⁸⁹ however, so far the concept lacks much substance, and even the OECD principles are of a high level of abstraction.¹⁹⁰

Since the adoption of the GDPR, the European Commission seems to have adopted its own approach to assessing adequacy, though there is little transparency about the methodology it uses.¹⁹¹ The adequacy decisions adopted since entry into force of the GDPR¹⁹² evidence the following approach by the Commission. First of all, decisions tend to consist of two major parts: (1) an assessment of ‘the rules applying to the processing of personal data’ which considers the legal framework surrounding the use of personal data, including any constitutional protection or international commitments; and (2) an assessment of governmental

¹⁸⁴ Ibid., p. 8.

¹⁸⁵ Ibid., p. 9.

¹⁸⁶ EDPB 2020A. See the commentary on Art. 46 in this edition.

¹⁸⁷ EDPB 2024B, p. 5.

¹⁸⁸ OECD 2022, pp. 7-8.

¹⁸⁹ See for example WEF 2020.

¹⁹⁰ Drechsler and Matsumi 2024, p. 145.

¹⁹¹ EDPB 2024B.

¹⁹² At the time of writing, these were Commission decision Japan 2019; Commission decision UK GDPR 2021; Commission decision Korea 2021; and Commission decision EU-US Data Privacy Framework 2023.

access and applicable remedies and supervision.¹⁹³ For the latter, the Commission distinguishes governmental access by law enforcement from access by national security agencies. Despite the CJEU requiring an assessment of the law in action (see the discussion of *Schrems I* and *Schrems II* above), adequacy assessments as documented in the recitals of the decisions usually do not make references to empirical studies or other sources of information that could give an impression of how a legal system works on the ground, and, at the most, include statistical information, e.g. on how often a particular remedy against governmental access was used in a certain year.¹⁹⁴ In the context of automated decision-making, except for the decisions covering the UK, the Commission has considered the likely effect of the absence of specific rules on the level of protection required,¹⁹⁵ though it reveals little about how it has done so.

4. Repeal, amendment or suspension of adequacy decisions

Adequacy as set out in Article 45 applies only when a formal Commission decision has been issued, i.e., it cannot be implied. The DPD also foresaw the possibility for the Commission to issue a decision finding that a third country did not provide an adequate level of protection,¹⁹⁶ but this was left out of the GDPR, nor has such a negative decision ever been issued under either the DPD or the GDPR.

Article 45 does contain detailed provisions dealing with situations where a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection after an adequacy decision has been issued. Such situations can arise when ‘information reveals’ that adequate protection no longer applies, which is to be broadly interpreted (e.g., it also includes situation when such information becomes known through reports in the news media). When this occurs, the Commission must repeal, amend or suspend its adequacy decision by means of an implementing act under the examination procedure referred to in Article 93(2),¹⁹⁷ except for ‘duly justified imperative grounds of urgency’, in which case the Commission must ‘adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3)’.¹⁹⁸ Article 45(5) says that the Commission ‘shall’ take such actions, so it has a duty to do so in such situations. Repeal or suspension of an adequacy decision could be seen as the functional equivalent of a negative adequacy decision, since it will require the Commission to declare formally that adequacy no longer exists.

Repeal, amendment or suspension of an adequacy decision shall not have retroactive effect,¹⁹⁹ which is a departure from normal EU law, since generally when an EU act is annulled, it disappears from the EU legal order from the date on which it entered into force (*ex tunc*).²⁰⁰ However, in cases involving ‘duly justified imperative grounds of urgency’²⁰¹ (which are not further defined), the Commission must adopt ‘immediately applicable implementing acts’ in accordance with the procedure under Article 93(3) GDPR. In its *Schrems II* judgment, the CJEU found that it can be appropriate to maintain the effects of an invalidated adequacy

¹⁹³ Commission decision Japan 2019; Commission decision UK GDPR 2021; Commission decision Korea 2021; Commission decision EU-US Data Privacy Framework 2023.

¹⁹⁴ See for example Commission decision UK GDPR, rec. 96.

¹⁹⁵ See for example Commission decision Korea, rec. 81.

¹⁹⁶ Art. 25(4) DPD.

¹⁹⁷ Art. 45(5) GDPR.

¹⁹⁸ Ibid.

¹⁹⁹ Ibid.

²⁰⁰ Lenaerts, Maselis and Gutman 2014, locations 18058–18065.

²⁰¹ Art. 45(5) GDPR.

decision if this necessary to avoid the creation of a ‘legal vacuum’, though it refused to do so in that case, and also did not define what a legal vacuum would be with regard to international data transfers.²⁰²

When the Commission repeals, amends or suspends an adequacy decision, it must enter into consultations with the third country or international organisation in order to remedy the situation.²⁰³ Such a decision is without prejudice to transfers of personal data carried out under Articles 46–49.²⁰⁴ This means that even if an adequacy decision is repealed by the Commission, data transfers to the affected third country or international organisation made pursuant to appropriate safeguards under Article 46, binding corporate rules under Article 47, or derogations under Article 49 are not affected.

5. Periodic review

The CJEU in *Schrems I* found that the Commission must check ‘periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified’.²⁰⁵ The GDPR requires that the implementing act determining adequacy provides for a periodic review at least every four years,²⁰⁶ though the review period may be shorter than this depending on the particular circumstances at hand.²⁰⁷ For example, the adequacy decision covering Japan foresees a first review two years after issuance and a periodic review every four years after that.²⁰⁸ In cases where incidents or changes in the legal framework of the third country or international organisations require it, a review may need to be conducted ahead of schedule.²⁰⁹

With regard to the procedure for conducting a periodic review, the GDPR states only that it should be ‘conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation’; that the Commission should ‘take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources’; and that the Commission should report ‘any relevant findings’ to the Committee established under Article 93.²¹⁰ In light of the CJEU’s findings in *Schrems I* that the Commission’s discretion in determining the adequacy of protection is ‘reduced’, and that its review of the adequacy requirements should be ‘strict’,²¹¹ a periodic review must be rigorous and comprehensive. The EDPB has stated that it expects to be kept informed of the review process and to participate in it.²¹²

²⁰² Case C-311/18, *Schrems II*, para. 202.

²⁰³ Art. 45(6) GDPR.

²⁰⁴ Art. 45(7) GDPR.

²⁰⁵ Case C-362/14, *Schrems I*, para. 76.

²⁰⁶ Art. 45(3) GDPR.

²⁰⁷ *Ibid.*, stating that the periodic review shall happen ‘at least’ every four years. See WP29 2018, p. 4.

²⁰⁸ Commission Decision Japan 2019, Art. 3(4). The first evaluation report of the Commission concerning the Japanese adequacy decision was published in 2023, and thus was two years late. See EC Report 2023.

²⁰⁹ WP29 2018, p. 4.

²¹⁰ See rec. 106 and the commentary on Art. 93 in this edition.

²¹¹ Case C-362/14, *Schrems I*, para. 78.

²¹² WP29 2018, p. 4.

Adequacy decisions of the Commission issued pre-GDPR also contained review clauses, though these were formulated more vaguely than under the GDPR.²¹³ The requirements of the GDPR concerning periodic review also apply to these previous adequacy decisions, so that the Commission must review them as well. At the time of writing, the Commission had published reviews for Japan and the EU-US Data Privacy Framework,²¹⁴ and must also publish a review of the UK adequacy decision due to the built-in sunset clause causing it to automatically terminate if it is not prolonged.²¹⁵

In 2024 the Commission published several years late its first evaluation report on the adequacy decisions issued under the DPD.²¹⁶ The report, accompanied by a lengthy staff working document with country reports,²¹⁷ concluded that each of the countries covered by the decisions continues to provide adequate protection. The working document reveals that the assessments were often based on recent reforms in the countries in question, suggesting that the Commission leveraged the threat of losing adequacy to push reforms. In a carefully worded letter, the EDPB highlights certain areas where the Commission could have provided more details, for example about how data subjects can exercise their rights in a third country and on the level of protection for automated decision-making.²¹⁸

In recent years a number of regional and international and regional groups have proposed or adopted rules to regulate international data transfers that may compete with the GDPR. For example, several countries have proposed ‘Global Cross-Border Privacy Rules’ (GCBPRs) as an alternative system for data transfers,²¹⁹ and regional groups such as ASEAN²²⁰ and the Ibero-American Data Protection Network²²¹ have published model contractual clauses for international data transfers. If third countries that are subject to a Commission adequacy decision allow transfers of data that they receive from the EU based on an alternative system, then it could put their adequacy decision in jeopardy.

6. Status of past adequacy decisions

Article 45(9) GDPR specifies that adequacy decisions previously issued under the DPD shall remain in force until amended, replaced or repealed by a Commission Decision as specified in this Article. Thus, existing adequacy decisions remain in effect under the GDPR. However, as explained above, they must be reviewed periodically as set out in Article 45(3).

7. Enforcement

A Commission adequacy finding is a ‘decision’ under Article 288 TFEU, the legality of which may only be reviewed by the CJEU, and is binding on all organs of Member States, including DPAs.²²² This means that, until an adequacy decision is declared invalid by the CJEU, Member

²¹³ See e.g. Commission Decision Argentina 2003 (Art. 4), Commission Decision Guernsey 2003 (Art. 5) and Commission Decision Israel 2011 (Art. 5), all stating merely that ‘The Commission shall monitor the functioning of this Decision’.

²¹⁴ EC Report 2023; EC Report 2024.

²¹⁵ Commission Decision UK GDPR, Art. 4.

²¹⁶ EC Report 2024.

²¹⁷ EC Commission Staff Working Document 2024.

²¹⁸ EDPB 2024B.

²¹⁹ See CBDPR Declaration.

²²⁰ See ASEAN Model Clauses.

²²¹ Iberoamerican Model Clauses.

²²² See also Case C-311/18, *Schrems II*, para. 117.

States and their organs cannot thwart the application of the decision, such as by adopting binding acts finding that the third country in question does not ensure an adequate level of protection.²²³ DPAs may also not suspend or prohibit data transfers based on the inadequacy of protection in a third country once an adequacy decision has been issued for it.²²⁴ However, a DPA may take such enforcement action for a different reason, such as that the data processing lacked a legal basis under Article 6 GDPR.²²⁵

The fact that adequacy decisions can only be reviewed by the CJEU, does not mean that individuals are without any remedies if they consider a decision invalid. As the CJEU clarified in the *Schrems I* judgment, an individual must still be able to make a claim to a DPA contesting the compatibility of a data transfer based on an adequacy decision, and the DPA must examine the claim with all due diligence.²²⁶ If it suspects that there is indeed a problem with the adequacy decision, then it must escalate the case to the CJEU.²²⁷ If the DPA rejects the claim, the individual must have access to judicial remedies allowing her to contest this decision before national courts, and the courts must stay proceedings and make a reference to the Court for a preliminary ruling.²²⁸

These requirements are reflected in provisions of the GDPR such as Articles 77 and 78, which give individuals the right to lodge a complaint against a DPA and to exercise an effective judicial remedy against one. In addition, under Article 58(2)(j) a DPA may order the suspension of data flows to a third country and international organisation, and Article 58(5) gives DPAs the power to bring infringements of the GDPR to the attention of judicial authorities and to engage in legal proceedings in order to enforce it. The important role of DPAs is also shown by the fact that while the CJEU in both *Digital Rights Ireland*²²⁹ and *Tele2*²³⁰ indicated that locating databases in third countries may raise fundamental rights issues, in *Opinion 1/15* Advocate General Mengozzi found that the retention of data outside the EU is not in itself problematic unless it ‘does not fully ensure a review of the requirements of protection and security by an independent authority’ (i.e. an EU-based DPA).²³¹

An adequacy decision can be challenged in the EU courts by individuals, who can bring an action for annulment under Article 263(4) TFEU. The General Court held inadmissible a claim brought by a not for profit company on behalf of itself and its members, supporters and the general public to seek annulment of the EU-US Privacy Shield,²³² but this was based on the lack of standing of the claimant in this case. A similar challenge launched by a French individual against the Data Privacy Framework is still pending, although an interim decision has rejected the request for immediate suspension.²³³ In addition, repeal or suspension of an adequacy decision by the Commission could arguably be challenged by a third country before the EU courts under Article 263 TFEU.²³⁴

²²³ Ibid., para. 118.

²²⁴ EDPB 2021C, p. 12 footnote 34.

²²⁵ Ibid.

²²⁶ Case C-362/14, *Schrems I*, para. 63.

²²⁷ EDPB 2020A, p. 5.

²²⁸ Case C-362/14, *Schrems I*, para. 64.

²²⁹ See Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, para. 68.

²³⁰ See Joined Cases C-203/15 and C-698/15, *Tele2*, para. 122.

²³¹ *Opinion 1/15* (AG Opinion), para. 277.

²³² Case T-670/16, *Digital Rights Ireland*.

²³³ Case T-553/23 R, *Phillipe Latombe v European Commission* (pending).

²³⁴ See Yovanof 2022.

Infringements of Articles 44–49 are subject to the higher level of administrative fines under Article 83(5)(c) GDPR, i.e. up to € 20 million or 4 per cent of the total worldwide turnover of the preceding financial year, whichever is higher.

Select Bibliography

International instruments

Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS No. 108.

Convention 108+: Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data 2018, CM/Inf(2018)15-final.

EEA Agreement: Agreement on the European Economic Area, OJ 1994 L 1/3.

Trade and Cooperation Agreement UK 2020: Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part, OJ 2020 L 444/14.

EU legislation

Commission Decision 2016/2295: Commission Implementing Decision (EU) 2016/2295 of 16 December 2016 amending Decisions 2000/518/EC, 2002/2/EC, 2003/490/EC, 2003/821/EC, 2004/411/EC, 2008/393/EC, 2010/146/EU, 2010/625/EU, 2011/61/EU and Implementing Decisions 2012/484/EU, 2013/65/EU on the adequate protection of personal data by certain countries, pursuant to Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2016) 8353), OJ 2016 L 344/83.

Commission Decision Andorra 2010: Commission Decision of 19 October 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra, OJ 2010 L 277/27.

Commission Decision Argentina 2003: Commission Decision 2003/1731 of 30 June 2003 pursuant to Directive (EC) 95/46 of the European Parliament and of the Council on the adequate protection of personal data in Argentina, OJ 2003 L 168/19.

Commission Decision Canada 2006: Commission Decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency, 2006 OJ L 91/49.

Commission Decision Faroe Islands 2010: Commission Decision of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on the processing of personal data, OJ 2010 L 58/17.

Commission Decision Guernsey 2003: Commission Decision 2003/821 of 21 November 2003 on the adequate protection of personal data in Guernsey, OJ 2003 L 308/27.

Commission Decision Isle of Man 2004: Commission Decision 2004/411 of 28 April 2004 on the adequate protection of personal data in the Isle of Man, OJ 2004 L 151/1.

Commission Decision Israel 2011: Commission Decision 2011/61/EU of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, OJ 2011 L 27/39.

Commission Decision Japan 2019: Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, OJ 2019 L 76/1.

Commission Decision Jersey 2008: Commission Decision of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey, OJ 2008 L 138/21.

Commission Decision Korea 2021: Commission Implementing Decision (EU) 2022/254 of 17 December 2021 pursuant to Regulation 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Republic of Korea under the Personal Information Protection Act, OJ 2022 L 44/1.

Commission Decision New Zealand 2013: Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand, OJ 2013 L 28/12.

Commission Decision PIPEDA 2002: Commission Decision (EC) 2002/2 of 20 December 2001 pursuant to Directive (EC) 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, OJ 2002 L 2/13.

Commission Decision Privacy Shield 2016: Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ 2016 L 207/1 (annulled).

Commission Decision Switzerland 2000: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, OJ 2000 L215/1.

Commission Decision UK GDPR 2021: Commission Implementing Regulation (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, OJ 2021 L 360/1.

Commission Decision UK LED 2021: Commission Implementing Decision (EU) 2021/1773 of 28 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, OJ 2021 L 360/69.

Commission Decision Uruguay 2012: Commission Implementing Decision of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data, OJ 2012 L 227/11.

Commission Decision EU-US Data Privacy Framework 2023: Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, OJ 2023 L 231/118.

EUDPR: 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 (Text with EEA relevance), OJ 2018 L 295/39.

GDPR: 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) (Text with EEA relevance), OJ 2016 L 119/1.

Safe Harbour 2000: European Commission Decision 2000/520 of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000 L 215/7 (annulled).

Umbrella Agreement US: Agreement on the Protection of Personal Information Relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses, OJ 2017 L 336/3.

National legislation

German GDPR Implementation Law: Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DsAnpUG-EU), BGBl 2017 Teil I Nr. 44.

Academic writings

Chander and Schwartz 2023: Anupam Chander and Paul Schwartz, ‘Privacy and/or Trade’, 90(1) *The University of Chicago Law Review* (2023), pp. 49-133.

Czerniawski 2024: Michal Czerniawski, ‘Shrouded in Secrecy – Does the Comitology Procedure for GDPR Adequacy Decisions Fit Its Purpose?’, 18(2) *Masaryk University Journal of Law and Technology* (2024), pp. 215-244

Docksey 2014: Docksey, ‘The European Court of Justice and the Decade of Surveillance’, in Hijmans and Kranenborg (eds.), *Data Protection Anno 2014: How to Restore Trust?* (Intersentia 2014), 97.

Docksey and Propp 2023: Docksey and Propp, ‘Government Access to Personal Data and Transnational Interoperability: An Accountability Perspective’, 10 *Oslo Law Review* (2023), 1.

Drechsler 2022: Drechsler, *Data subject rights in international personal data transfers* (Dissertation Vrije Universiteit Brussel, 2022).

Drechsler 2024: Drechsler, ‘Article 36’, in Kosta and Boehm (eds.), *The EU Law Enforcement Directive (LED): A Commentary* (OUP 2024), 373 (electronic edition).

Drechsler and Matsumi 2024: Laura Drechsler and Hideyuki Matsumi, ‘Caught in the middle: The Japanese approach international personal data flows’, 14(2) *International Data Privacy Law* (2024), pp. 134-149.

Koutrakos 2018: Koutrakos, ‘The Decision-Making Process’, in Schütze and Tridimas (eds.), *Oxford Principles of European Union Law* (OUP 2018), 1141 (electronic edition).

Lenaerts, Maselis and Gutman 2014: Lenaerts, Maselis and Gutman, *EU Procedural Law* (OUP 2014) (Kindle edition).

Marelli 2024: Marelli, ‘Transferring personal data to international organizations under the GDPR: an analysis of the transfer mechanisms’, 14 *International Data Privacy Law* (2024), 19.

Ntouvas 2019: Ntouvas, ‘Exporting personal data to EU-based international organizations under the GDPR’, 9 *International Data Privacy Law* (2019), 272.

Schantz 2023: Schantz, ‘Article 45’, in Spiecker genannt Döhmann, Papakonstantinou, Hornung and De Hert (eds.), *General Data Protection Regulation: Article-by-Article Commentary* (Beck/Hart/Nomos 2023), 785 (Kindle edition).

Simitis and Dammann 1997: Simitis and Dammann, *EU-Datenschutzrichtlinie* (Nomos-Verlag 1997).

Stoddart, Chan and Joly 2016: Stoddart, Chan and Joly, ‘The European Union’s Adequacy Approach to Privacy and International Data Sharing in Health Research’, 44(1) *The Journal of Law, Medicine & Ethics* (2016), 143.

Yakovleva 2024: Yakovleva, *Governing Cross-Border Data Flows: Reconciling EU Data Protection and International Trade Law* (OUP 2024).

Yovanof 2022: Yovanof, ‘The ECJ and the rise of adjudicatory jurisdiction: *Venezuela v Council*’, 59 *Common Market Law Review* (2022), 1893.

Papers of data protection authorities

EDPB Endorsement: European Data Protection Board, ‘Endorsement 1/2018’ (25 May 2018).

EDPB 2018: European Data Protection Board, 'Opinion 28/2018 Regarding the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data in Japan' (5 December 2018).

EDPB 2020A: European Data Protection Board, 'Recommendations 02/2020 on the European Essential Guarantees for surveillance measures' (10 November 2020).

EDPB 2020B: European Data Protection Board, 'Guidelines 2/2020 on articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies' (Version 2.0, 15 December 2020).

EDPB 2021A: European Data Protection Board, 'Statement 04/2021 on international agreements including transfers' (13 April 2021).

EDPB 2021B: European Data Protection Board, 'Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom' (13 April 2021).

EDPB 2021C: European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' Version 2.0 (18 June 2021).

EDPB 2021D: European Data Protection Board, 'Opinion 32/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic Korea' (24 September 2021).

EDPB 2023A: European Data Protection Board, 'Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework' (28 February 2023).

EDPB 2023B: European Data Protection Board, 'Report of the work undertaken by the supervisory authorities within the 101 Task Force' (28 March 2023).

EDPB 2023C: European Data Protection Board, 'Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook services (Art. 65 GDPR)' (13 April 2023).

EDPB 2024A: European Data Protection Board, 'Guidelines 01/2023 on Article 37 Law Enforcement Directive' (Version 2.1, 19 June 2024).

EDPB 2024B: European Data Protection Board, 'EDPB letter to the European Commission on its review of its eleven adequacy decisions adopted under Directive 95/46/EC' (5 December 2024).

EDPS 2016: European Data Protection Supervisor, 'Opinion 1/2016: Preliminary Opinion on the Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offences' (12 February 2016).

EDPS 2024: European Data Protection Supervisor, 'EDPS Investigation into Use of Microsoft 365 by the European Commission (Case 2021-0518)' (8 March 2024).

WP29 1998: Article 29 Working Party, 'Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive' (WP 12, 24 July 1998).

WP29 2012: Article 29 Working Party, 'Opinion on the level of protection of personal data in the Principality of Monaco' (WP 198, 19 July 2012).

WP29 2018: Article 29 Working Party, 'Adequacy Referential (updated)' (WP 254, 6 February 2018).

DPC 2023: Data Protection Commissioner, 'In the matter of Meta Platforms Ireland Limited (previously known as Facebook Ireland Limited)' (IN-20-8-1, 12 May 2023).

Dutch DPA 2024: Autoriteit Persoonsgegevens, ‘Besluit tot oplegging bestuurlijke boete: Uber Technologies Inc. en Uber B.V.’ (22 July 2024).

Reports and recommendations

ASEAN Model Clauses: ASEAN Model Contractual Clauses for Cross Border Data Flows (2021).

CBDPR Declaration: U.S. Department of Commerce, ‘Cross-Border Data Privacy Rules Declaration’ (2022).

Council Position on GDPR Evaluation 2023: Council of the European Union, ‘Council position and findings on the application of the GDPR’, no. 13538/23 (4 October 2023).

EC Communication 2017: Communication from the Commission to the European Parliament and the Council, ‘Exchanging and Protection Personal Data in a Globalised World’, COM(2017) 7 final, 10 January 2017.

EC Communication 2020: European Commission, ‘Communication from the European Commission to the European Parliament and the Council: Data Protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition—two years’ of application of the General Data Protection Regulation’, COM(2020) 264 final (24 June 2020).

EC Communication 2024: European Commission, ‘Communication from the Commission to the European Parliament and the Council: Second Report on the application of the General Data Protection Regulation’, COM(2024) 357 final, 25 July 2024.

EC Report 2023: Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decision for Japan, COM(2023) 275 final, 3 April 2023.

EC Report 2024: Report from the Commission to the European Parliament and the Council on the first periodic review of the functioning of the adequacy decision on the EU-US Data Privacy Framework, COM(2024) 451 final, 9 October 2024.

EP Resolution 2000: European Parliament resolution on the draft Commission decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce (C5-0280/2000—2000/2144(COS)), 5 July 2000.

EP Resolution 2018: European Parliament; ‘European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield’ (P8_TA-PROV(2018)0315), 5 July 2018).

EP Resolution 2023: European Parliament, ‘European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP))’ (P9_TA(2023)0204, 11 May 2023).

European Ombudsman 2023: European Ombudsman, Case 201/2022/JK, 31 October 2023.

Iberoamerican Model Clauses: Red Iberoamericana de Protección de Datos, Guía de Implementación de Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales (TIDP) (2022).

Multistakeholder Expert Group Report 2024: Commission Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679, ‘Report: Contribution from the Multistakeholder Expert Group to the Commission 2024’ (10 June 2024).

OECD 2022: OECD, ‘Declaration on Government Access to Personal Data Held by Private Sector Entities’ (2022).

WEF 2020: World Economic Forum, ‘White Paper: Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows’ (2020).

Others

Christakis, Felz and Swire 2024: Theodore Christakis, Dan Felz, and Peter Swire, ‘German court decision signals move towards risk-based approach to data transfers’, *Cross-Border Data Forum* (16 October 2024).

Hanke 2017: Hanke, 'EU Trade, the Martin Selmayr Way', <I>POLITICO</I> (7 November 2017), available at <https://www.politico.eu/article/eu-trade-the-martin-selmayr-way/>.

Ihle 2010: Ihle, 'Ireland Blocks EU Data Sharing with Israel', <I>JTA</I> (8 July 2010), available at <http://www.jta.org/2010/07/08/news-opinion/world/ireland-blocks-eu-data-sharing-with-israel>.

Lenaerts speech 2018: Lenaerts, 'The EU General Data Protection Regulation Five Months On', speech by CJEU President Koen Lenaerts at the 40th International Conference of Data Protection and Privacy Commissioners (25 October 2018), available on YouTube.

Noyb Website Data Transfers: noyb, 'Data transfers', available at <https://noyb.eu/en/project/eu-us-transfers>.

Article 61. Mutual assistance

*CHRISTOPHER DOCKSEY**

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.
2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.
3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.
4. The requested supervisory authority shall not refuse to comply with the request unless:
 - (a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or
 - (b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.
5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.
6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.
7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.
8. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).
9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

* This contribution is based on the first edition of the Commentary, the author of which was Peter Blume, and on the update, the author of which was Christopher Docksey.

Relevant Recitals

(123) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.

(133) The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. A supervisory authority requesting mutual assistance may adopt a provisional measure if it receives no response to a request for mutual assistance within one month of the receipt of that request by the other supervisory authority.

(138) The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism.

CLOSELY RELATED PROVISIONS

Article 50 (International cooperation) (see too recital 116); Article 51(2) (Obligation of supervisory authorities to cooperate to ensure consistency) (see too recital 124); Article 56 (Competence of lead supervisory authority) (see too recitals 124–128); Article 57(1)(g) (Tasks of supervisory authorities); Article 60 (Cooperation between lead supervisory authority and supervisory authorities concerned) (see too recitals 130–31); Article 62 (Joint operations of DPAs) (see too recital 134); Article 64(2) (Opinion of the Board in case of non-compliance with Articles 61 or 62) (see too recital 136); Article 66 (request for an urgent binding decision from the Board).

RELEVANT CASE LAW

CJEU

Case C-503/03, *Commission of the European Communities v Kingdom of Spain*, judgment of 31 January 2006 (Grand Chamber) (ECLI:EU:C:2006:74).

Case C-230/14, *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, judgment of 1 October 2015 (ECLI:EU:C:2015:639).

Case C-507/17, *Google v Commission nationale de l'informatique et des libertés (CNIL)*, judgment of 24 September 2019 (ECLI:EU:C:2019:772).

Case C-645/19, *Facebook Ireland and others v Gegevensbeschermingsautoriteit*, judgment of 15 June 2021 (Grand Chamber) (ECLI:EU:C:2021:483).

Opinion of Advocate General Bobek in Case C-645/19, *Facebook Ireland Limited, Facebook Inc., Facebook Belgium BVBA v Gegevensbeschermingsautoriteit*, delivered on 13 January 2021 (ECLI:EU:C:2021:5).

Case C-184/20, *OT v VTEK (Chief Official Ethics Commission)*, judgment of 1 August 2022 (ECLI:EU:C:2022:601).

Case C-154/21, *RW v Österreichische Post*, judgment of 12 January 2023 (ECLI:EU:C:2023:3).

Case C-252/21, *Meta Platforms v Bundeskartellamt*, judgment of 4 July 2023 (ECLI:EU:C:2023:537).

Case C-46/23, *Újpesti Polgármesteri Hivatal v NAIH*, judgment of 14 March 2024 (ECLI:EU:C:2024:239).
Joined Cases T-70/23, T-84/23 and T-111/23, *Data Protection Commission v European Data Protection Board*, judgment of 29 January 2025 (ECLI:EU:T:2025:116).

A. Rationale and Policy Underpinnings

Article 61 GDPR concerns cooperation between supervisory authorities by way of information exchange and mutual assistance. Its general purpose is to contribute to the correct and consistent implementation and application of the GDPR, in particular, but not exclusively, as part of the ‘one-stop-shop’ mechanism laid down by Article 60 GDPR. This mechanism is intended to ensure uniform supervision of controllers and processors that conduct cross-border processing of personal data and to ensure the consistent application of the GDPR throughout the EU and EEA. Under this mechanism, a company operating in two or more Member States normally has one supervisory authority — termed as ‘lead supervisory authority’ (LSA) by the GDPR — as its sole interlocutor with regard to data protection compliance matters.¹

Article 61 applies in cases where one DPA formally requests information or mutual assistance measures from another DPA.

The rules set out in Article 61 complemented those in Article 60(2), which provides that the ‘lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 ... , in particular for ... monitoring the implementation of a measure concerning a controller or processor established in another Member State’.²

B. Legal Background

1. EU legislation

Article 61 has limited antecedents under Article 28(6) DPD, the single binding provision dealing with cooperation between European DPAs. This provided that: ‘The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information’. Recital 64 DPD explained that ‘the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union’. Under this previous EU framework, supervisory authorities cooperated by exchanging information and providing assistance on an informal basis in specific cases.

The implementation of Article 28(6) DPD was generally seen as problematic.³ Research concluded that ‘cooperation among DPAs has been taking place for a long time. This cooperation has been characterised for being irregular, heterogeneous and often based on questions of geographical proximity and trust’.⁴ DPAs reported that ‘exchanges of information have been taking place in the context of activities of a very different nature and DPAs have informed about the wide plethora of types of information that they share, including plans and intentions, case law, decisions, experiences and best practices, informal thinking, opinions, and requests for opinions’.⁵

¹ See the commentary on Art. 56 in this edition.

² See the commentary on Art. 60 in this edition.

³ See WP29 2011.

⁴ Papakonstantinou 2016, p. 65.

⁵ Barnard-Wills and Wright 2015, p. 16.

In practice, the main multilateral forum for EU DPAs to exchange information was the former WP29, now the EDPB, where DPAs and their staff meet regularly in the plenary and the expert subgroups (ESG), such as the Cooperation, Enforcement and Strategic Advisory subgroups.⁶ In this context the EDPB has sometimes established a task force to enable DPAs, in their enforcement role, to share information and coordinate national positions on a specific issue.⁷ The resulting reports reflect the common denominator agreed by the participating DPAs, without prejudice to determinations by DPAs in specific cases, and do not represent the position of the Board itself.⁸

Other European fora for the exchange of experience and information are the European Conference of Data Protection Authorities ('Spring Conference'), the Council of Europe Consultative Committee on the protection of personal data, and linguistic and regional fora such as the BIIDPA (British, Irish and Islands' Data Protection Authorities), the cooperation among Nordic DPAs, the Central Eastern European Data Protection Authorities ('CEEDPA') and the Conference of Balkan Data Protection Authorities.⁹

As the GDPR provides for a higher degree of harmonisation, DPAs have had to increase the intensity of their cooperation, and Article 61 lays down a specific, mandatory framework for formal cooperation. In this respect, the LED, the EPD and the EUDPR also provide for forms of cooperation between supervisory authorities.

Article 50 LED addresses mutual assistance between supervisory authorities in the law enforcement area. Many of these authorities will also be the supervisory authorities under the GDPR. As the LED is a directive, its mutual assistance provisions, unlike those in the GDPR, have to be implemented by Member States. In substance, these two components of the data protection reform package are aligned on mutual assistance, although the procedural context is quite different. As national police forces are responsible within their jurisdiction solely to the competent authority of that jurisdiction, the LED lacks the enforcement provisions of the consistency mechanism and, in particular, the urgency procedure available under Article 61(8) GDPR.¹⁰

Article 15a(4) EPD provides for cross-border cooperation by empowering the relevant data protection or telecoms regulators to 'adopt measures to ensure effective cross-border cooperation in the enforcement of the national laws adopted pursuant to this Directive and to create harmonised conditions for the provision of services involving cross-border data flows'.

Finally, Article 61 EUDPR requires the EDPS to cooperate with national supervisory authorities¹¹ 'to the extent necessary for the performance of their respective duties, in particular

⁶ Established under Art. 25 EDPB Rules of Procedure. Current work of the ESG can be seen on each meeting agenda of the EDPB. Thirteen ESG were listed on the EDPB website at the time of writing, see EDPB Subgroups & Taskforces.

⁷ E.g. the drafting of the WP29 2013 and the taskforce on the UBER data breach case established by the WP29 in 2017. More recent examples include the Cookie Banner Taskforce Report, the Supervisory Authorities Report and the ChatGPT Taskforce Report. Three Taskforces were listed on the EDPB website at the time of writing, see EDPB Subgroups & Taskforces.

⁸ See the Disclaimers in the above Reports of 2023 and 2024.

⁹ See Papakonstantinou 2016, pp. 65–66.

¹⁰ See Caruana 2024, pp. 705 and 709.

¹¹ The EDPS also cooperates with national supervisory authorities within the Customs Information System Supervision Coordination Group (CIS SCG) which ensures coordinated supervision of data protection in the Customs Information System.

by providing each other with relevant information, asking each other to exercise their powers and responding to each other's requests'.

Article 62 EUDPR goes on to regulate the coordinated supervision by the EDPS and national supervisory authorities of law enforcement bodies¹² and EU large-scale information systems,¹³ which it places within the framework of the EDPB. To this effect the Board has set up a Coordination Supervision Committee (CSC), which bring together the EDPS and the DPAs of EU Member States and of non-EU Members of the Schengen Area when required.¹⁴

In this respect, Article 44 of Europol Regulation 2016/794, as amended in 2022,¹⁵ provides that the EDPS should act in close cooperation with national supervisory authorities on issues requiring national involvement, in particular with regard to the use of Europol's channels of information, again within the framework of the EDPB.¹⁶

Finally, Article 51 EUDPR requires the EDPS, in cooperation with the Commission and the EDPB, to take appropriate steps to ensure international cooperation for the protection of personal data.

2. International instruments

Article 13(3)(b) of Convention 108 lays down an obligation of mutual assistance. Designated authorities are required to 'take, in conformity with . . . domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed'. Article 1(5) of the Additional Protocol¹⁷ adds the obligation on supervisory authorities, 'without prejudice' to Article 13 of the Convention, to 'co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information'.

Once it enters into force, Convention 108+ will strengthen these provisions in the new Chapter V on cooperation and mutual assistance. Article 17(1)(a) makes explicit the duty to provide mutual assistance by exchanging information and cooperating and adds in subparagraph (b) the obligation of 'coordinating . . . investigations or interventions, or conducting joint actions'. Article 17(2) provides that the 'information referred to in paragraph 1 shall not include personal data undergoing processing unless such data are essential for co-operation, or where the data subject concerned has given explicit, specific, free and informed consent to its provision'. Finally, Article 17(3) provides that, in order to organise their cooperation and to perform their duties, supervisory authorities should 'form a network'. Article 20 specifies that a request for mutual assistance may not be refused save for specific institutional reasons, namely

¹² Presently the EU Agency for Criminal Justice Cooperation (Eurojust), the European Public Prosecutor's Office (EPPO), and the EU Agency for Law Enforcement Cooperation (Europol).

¹³ Presently the Internal Market Information System (IMI) and the Schengen Information System (SIS).

¹⁴ Art. 37, EDPB Rules of Procedure. See Caruana 2024 pp. 702-703, and Gómez Navarro 2024, pp. 720-721. The participation may depend on whether the respective country applies the EU legal act establishing the large-scale IT system or the EU office, body or agency.

¹⁵ Regulation 2016/794.

¹⁶ The CSC has taken over the tasks of an earlier model of cooperation concerning Europol, the Europol Cooperation Board (ECB), since the Europol Regulation was amended in 2022. The ECB was a cooperation board with an advisory function referred to in recital 78 EUDPR, providing for cooperation between the EDPS, as the supervisory authority of Europol, and national supervisory authorities.

¹⁷ Additional Protocol Convention 108.

incompatibility with the powers of the requested authority, with the provisions of Convention 108+, or with the sovereignty, national security, public order or rights and freedoms of individuals in the requested Party.

In the international context,¹⁸ the two most important fora where EU DPAs are able to exchange information and experiences with third party DPAs are the Global Privacy Assembly ('GPA'),¹⁹ formerly known as the International Conference of Data Protection and Privacy Commissioners ('ICDPPC'), and the Global Privacy Enforcement Network ('GPEN').²⁰ Two documents adopted under the framework of the ICDPPC may be noted. First, the *International Standards on the Protection of Personal Data and Privacy*, which provided that supervisory authorities should '(s)hare reports, investigation techniques, communication and regulatory strategies and any other useful information for exercising their functions more effectively, in particular following a request for cooperation by another supervisory authority in conducting an investigation or intervention'.²¹ Secondly, the *Global Cross Border Enforcement Cooperation Arrangement*, which included the identification of 'possible issues or incidents for coordinated action and the active seeking of opportunities to coordinate cross-border actions where feasible and beneficial amongst the elements for the coordination of cross border enforcement activities'.²²

Finally, individual EU/EEA DPAs may have specific international agreements in place regarding mutual assistance and the exchange of information, comparable to the informal mutual assistance between European DPAs discussed below.²³

3. Case law

The CJEU has established in consistent case law on the supervisory authorities' powers and duty to cooperate under the DPD that cooperation is an active, not a passive obligation. Most recently it has specifically considered Article 61 GDPR itself, where it has emphasised the indispensable nature of dialogue and sincere and effective cooperation between the supervisory authorities concerned by a case.²⁴

In *Commission v Spain*, the Court considered the automatic implementation, without further investigation or information, of an alert under the Schengen Agreement. The Court found that

¹⁸ See Papakonstantinou 2016, pp. 66–67.

¹⁹ The purposes of the GPA are, inter alia, to promote and enhance internationally personal data protection, to draft and adopt joint resolutions and to encourage and facilitate cooperation and the exchange of information.

²⁰ The GPEN is an informal network of DPAs which enables sharing of best practice, cooperation and support and coordinates an annual 'Privacy Sweep' to understand industry practice and compliance on specific privacy issues. It was inspired by OECD Recommendation 2007, which called on OECD member economies to 'foster the establishment of an informal network . . . to discuss the practical aspects of privacy law enforcement co-operation, share best practices . . . work to develop shared enforcement priorities, and support joint enforcement initiatives and awareness raising campaigns'. See OECD Recommendation 2007 and GPEN Website.

²¹ ICDPPC 2009, Art. 2(a).

²² ICDPPC 2017, Chapter 8, Coordination Principles, section (i). See the commentary on Art. 50 in this edition for more detail on international cooperation.

²³ See for example the Memorandum of Understanding of 25 July 2019 between the U.S. Federal Trade Commission and the Dutch DPA on mutual assistance in the enforcement of laws protecting personal information in the private sector.

²⁴ Case C-645/19, *Facebook Ireland and others*, paras. 63 and 64. See too Joined Cases T-70/23, T-84/23 and T-111/23, *DPC v EDPB*, para. 53.

the principle of ‘genuine cooperation’ underpinning the Schengen *acquis* required the provision of supplementary information to enable the case to be correctly assessed.²⁵

In *Weltimmo*, the CJEU considered the situation of the Hungarian and Slovakian supervisory authorities with regard to a company registered in Slovakia which exclusively conducted its activities in Hungary. The CJEU underlined the necessity for cooperation under Article 28(6) DPD and emphasised that enforcement cooperation is an obligation for the requested supervisory authority, which ‘may, in the context of that cooperation, find it necessary to carry out other investigations, on the instructions of the [requesting] supervisory authority’.²⁶

The Court has specifically considered Article 61 GDPR in *Facebook Ireland*, following in part the detailed analysis by Advocate General Bobek. This case concerned the competence of the LSA under Article 56 GDPR in the context of the consistency mechanism and the one-stop-shop. The Court confirmed that an LSA has in principle the sole competence to initiate or engage in legal proceedings against the controller,²⁷ but stressed that Article 56(1) requires ‘close, sincere and effective cooperation’ between the DPAs concerned and that the LSA ‘cannot eschew essential dialogue with and sincere and effective cooperation with the other supervisory authorities concerned’.²⁸ The Advocate General emphasised the need to ensure consistency and prevent the risk of fragmentation under the DPD whereby various DPAs may take different approaches with regard to cross-border processing.²⁹

C. Analysis

1. Introduction

One of the main objectives of the GDPR is its effective and consistent application and enforcement throughout the EU/EEA, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. To this end, the GDPR lays down specific rules to ensure that mutual assistance and cooperation are implemented in practice, based on specific procedural steps. In essence, cooperation is made mandatory following a request for assistance, subject to very limited grounds for refusal and to specific consequences for failure to cooperate.

Article 61 falls within the innovative GDPR procedures for cross-border cases in Chapter VII, in particular the cooperation mechanism between supervisory authorities in Section 1 thereof (the so-called ‘one-stop-shop’) as well as other forms of cooperation. It establishes a binding mechanism for mutual assistance between EU and EEA supervisory authorities, including, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.³⁰

²⁵ Case C-503/03, *Commission v Spain*, para. 56.

²⁶ Case C-230/14, *Weltimmo*, para. 58.

²⁷ Subject to specific exceptions, such as local cases under Art. 56(2) and the urgency procedure under Art. 66, see Case C-645/19, *Facebook Ireland and others* (AG Opinion), paras. 57-59.

²⁸ Case C-645/19, *Facebook Ireland and others*, para. 63.

²⁹ Case C-645/19, *Facebook Ireland and others* (AG Opinion), paras. 76-80.

³⁰ Note that the EDPB itself may order a national supervisory authority to carry out further investigations in the context of an Article 65 dispute settlement procedure. See Joined Cases T-70/23, T-84/23 and T-111/23, *DPC v EDPB*. See further the commentary on Art. 65 in this edition.

Article 61 should be considered alongside five other provisions of the GDPR which require DPAs to cooperate so as to ensure consistency of application and enforcement under the GDPR:

1. Article 57(1)(g) requires national DPAs to cooperate with other supervisory authorities, including sharing information and providing mutual assistance;
2. Article 60 lays down the one-stop-shop cooperation mechanism, whereby Article 60(2) provides that an LSA may request the concerned supervisory authorities (CSAs) to provide relevant information and mutual assistance pursuant to Article 61, and Article 60(3) requires the LSA to communicate the relevant information on the matter without delay to the CSAs. Such cooperation is essential in the context of cross-border enforcement as each national supervisory authority remains competent to carry out investigations on the territory of its Member State;³¹
3. Article 62 requires supervisory authorities to conduct, where appropriate, joint operations including joint investigations and joint enforcement measures;
4. Article 66 lays down an urgency procedure related in part to failure to respond to a request for mutual assistance under Article 61; and
5. Article 50(1)(b) requires the Commission and supervisory authorities to take appropriate steps to ‘provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange’.

In practice, the formal cooperation procedure laid down in Article 61 is used mainly when other forms of voluntary cooperation are deemed insufficient in light of the enforcement needs at issue. This role of Article 61 in strengthening enforcement cooperation has been incorporated into the proposed Procedural Regulation, which at the time of writing is in the trilogue stage. The Proposal emphasises the need for DPAs to endeavour to reach consensus at an early stage on the scope and assessment of the factual and legal elements of a complaint. Under Article 10 of the Proposal, where a CSA disagrees with the assessment of an LSA, both the Commission proposal and the Parliament’s text require the CSA to use mutual assistance under Article 61 GDPR and joint operations under Article 62 GDPR. The Council retains this positive approach to Articles 61 and 62 GDPR, but allows DPAs the option of submitting the request for mutual assistance or joint operations.³²

2. The formal mutual assistance procedure

Article 61 is ‘one of the mechanisms for supervisory authorities to ensure proper and efficient cooperation’³³ so that the GDPR is applied effectively and consistently across the EU/EEA. According to recital 123, cooperation is the duty of each individual DPA, as also underlined in recital 133. Article 61 lays down a formal cooperation procedure which, once triggered by a requesting DPA, is mandatory for the DPA which receives the request. As outlined further below, this formal cooperation is different from — but complementary to — other forms of voluntary mutual assistance that are available to DPAs.

Paragraph 1 of Article 61 requires supervisory authorities to provide each other with relevant information and mutual assistance, in order to implement and apply the GDPR in a consistent manner throughout the EU/EEA, and to put in place measures for effective cooperation with one another. It then sets out the scope of mutual assistance in an illustrative and non-exhaustive

³¹ See Art. 55(1) and rec. 130 GDPR.

³² Trilogue table, Art. 10(1) and Art. 10(1)(b).

³³ EDPB 2023A, para. 236.

(‘in particular’) list of elements that may be requested, namely ‘information ... and ... prior authorisations and consultations, inspections and investigations’. The substantive final element of ‘investigations’ replaced the informational final elements of the list in Article 55(1) of the original Commission Proposal, now Article 61(1) GDPR (‘prompt information on the opening of cases and ensuing prompt information on the opening developments where data subjects in several Member States are likely to be affected by processing operations’).

Paragraph 2 of Article 61 specifies the deadline to be respected and includes a non-exhaustive example of measures that the requested authority may take to reply to a request (‘the transmission of relevant information on the conduct of an investigation’). When a DPA makes a request for help, the requested DPA must answer without undue delay and at the latest within a month after receiving the request. Under Article 61(8) the deadline of one month is integrated into the consequences of failure to respond to the request within that deadline, namely the adoption of provisional measures by the requesting authority. The Board has stressed that only requests under the formal mutual assistance procedure laid down in Article 61 may trigger these consequences.³⁴ Article 55(2) of the Commission Proposal, now Article 61(2) GDPR, included a second example of possible measures (‘enforcement measures to bring about the cessation or prohibition of processing operations contrary to this Regulation’) which was not retained.

Paragraph 3 of Article 61 requires the request to contain all the necessary information, including the purpose of and reasons for the request. The case in question must accordingly be described in sufficient detail to enable the requested authority to comply with the request, or to refuse to do so. The purpose sets the limits of the request, as paragraph 3 expressly limits the use of information exchanged to the purpose for which it was requested.

Paragraph 4 of Article 61 provides that the requested supervisory authority may only refuse to comply with the request if it is not the competent authority or if compliance would contradict provisions of the GDPR, EU law or the national law to which the requested DPA is subject.

Paragraph 5 of Article 61 provides that the requested supervisory authority must inform the requesting supervisory authority of the results or the progress of the measures it has taken in order to respond to the request. This is an obligation of information, however, since Article 61(5) does not require the requested authority to take action.³⁵ Under the second sentence of this provision, the requested DPA must substantiate the reasons for any rejection of the request.

Paragraph 6 of Article 61 requires requested supervisory authorities, as a rule, to supply the information requested by other supervisory authorities by electronic means, using a standardised format. This requirement can also be seen in Articles 60(12) and 64(4). Article 61(9) and Article 67 empower the Commission to adopt delegated legislation to specify the arrangements for the exchange of information by electronic means, including the standardised

³⁴ In 2021 the EDPB rejected a request for corrective measures made in the context of voluntary mutual assistance, see EDPB 2021, paras. 177-178. See also EDPB 2023A, para. 228.

³⁵ Papakonstantinou 2023, pp. 920-921.

format to be used.³⁶ On this basis the Commission adopted the ‘IMI Implementing Act’³⁷ providing for the use of the Internal Market Information system (IMI) for GDPR consistency and cooperation procedures, including Article 61 GDPR mutual assistance requests.

Paragraph 7 of Article 61 generally precludes requested supervisory authorities from charging a fee for any action taken by them pursuant to a request for mutual assistance. In exceptional circumstances supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance, but there do not appear to have been any examples of this.

3. Provisional measures, local enforcement and escalation to the EDPB

Paragraph 8 of Article 61 addresses the situation where a requested DPA fails to inform the requesting authority of the results of, or measures taken to respond to, the request. In this case, the requesting authority may take provisional measures within its own Member State, pursuant to the normal rule of competence under Article 55(1).

Article 61(8) spans the first two sections of Chapter VII GDPR, namely Cooperation in Section 1 and Consistency in Section 2. The purpose of implementing and applying the GDPR in a consistent manner throughout the EU/EEA is common to Articles 61 and Article 63, the head article of the consistency mechanism, and the Court has consistently stressed that this purpose underlies both cooperation and consistency.³⁸ In effect, Article 61(8) is a bridge to the consistency mechanism in Section 2, which is designed to escalate the matter to EU level in exceptional cases of failure to cooperate under Section 1.

Thus, Article 61(8) further provides that if a request for assistance is not answered within a month, the requesting authority may adopt provisional measures under the urgency procedure under Article 66(1) in Section 2. In this case, the urgency is presumed, and an urgent binding decision by the EDPB under Article 66(2) may be requested without needing to demonstrate the urgent need to act, for example where the requesting authority considers that its adopted provisional measures are insufficient and a decision of the Board is necessary. At the time of writing there have been two urgent binding decisions by the EDPB, in one of which Article 61(8) was held to be applicable.³⁹

In the alternative, if a requested DPA does not comply with its obligations under Article 61, Article 64(2) provides that the requesting DPA may request that the matter be considered by the EDPB with a view to obtaining an opinion. Failure to respect such an opinion can then lead to a binding decision by the Board under Article 64(8) and Article 65(1)(c). Up to the time of writing, however, no such opinion under Article 64(2) has been requested.⁴⁰

³⁶ See the commentary on Art. 93 in this edition on the procedure to be followed by the Commission to specify the arrangements for the exchange of information by electronic means. See also the commentary on Art. 67 in this edition, which discusses the IMI system used by DPAs and the EDPB since the GDPR entered into application.

³⁷ Decision 2018/743.

³⁸ See Case C-507/17, *Google v CNIL*, para. 68; Case C-645/19, *Facebook Ireland*, para. 52; and Case C-252/21, *Meta Platforms v Bundeskartellamt*, para. 41.

³⁹ EDPB 2023A, paras. 235-257. Cf. EDPB 2021, paras. 176-180, in which the requesting authority failed to demonstrate that the LSA had failed to provide information in the context of a formal request for mutual assistance under Art. 61.

⁴⁰ See the commentary on Art. 66 in this edition, point C.2.1.2.

The experience of the two adopted urgent binding decisions demonstrates that Article 61 offers not only the ability to request mutual assistance, but also the possibility in exceptional cases of speeding up the process of cross-border enforcement. This experience also reveals a significant difference of views among DPAs as to the scope of Article 61. The Norwegian DPA and the Hamburg DPA have taken the broad view that it is possible for a CSA to submit a formal mutual assistance request that an LSA should impose corrective measures such as a ban or temporary ban on processing. In contrast the Irish DPA has taken the narrow view that the provisions of Article 61 are limited to the provision of information, and do not extend to requesting a temporary ban on processing by way of mutual assistance.⁴¹

The issue was discussed in *Facebook Ireland*, where the CJEU stressed that the obligations under Article 61 must be respected and Advocate General Bobek took a specific position on the scope of those obligations.

The Advocate General noted that the GDPR addresses ‘situations of administrative inertia’, in particular, where an LSA ‘fails to take any meaningful action in order to investigate possible breaches of the GDPR and, where appropriate, enforce its rules’⁴². In such situations he noted that CSAs could follow one of the two alternative routes, under Article 61 and Article 64(2), discussed above.⁴³ With regard to Article 61, he felt that a CSA may request an LSA to provide mutual assistance by way of ‘putting in place of measures for effective cooperation.’⁴⁴ A failure to react to such a request within the deadline ‘may thus enable the [CSA] to adopt the urgent measures considered necessary to protect the interests of data subjects.’⁴⁵

Relying on the argument that where there is an ‘urgent need to act to protect the rights of data subjects’ the ‘need to adopt an interim measure might present itself, for example, in case of failure to act of the lead supervisory authority’,⁴⁶ the Advocate General concluded that the Article 61 procedure is ‘probably meant to be used’ by a CSA vis-à-vis an LSA, to enable the CSA to adopt the urgent measures considered necessary to protect the interests of data subjects.⁴⁷

The CJEU, like the Advocate General, handed down a ruling that supported the special competence of the LSA in cross border cases under Article 56⁴⁸ and agreed that a CSA is competent to take action under either Article 61 or Article 64(2) where an LSA does not comply with its Article 61 obligations for mutual assistance. However, the Court left open the broad or narrow nature of the obligations imposed by Article 61 and limited itself to confirming the case under Article 61(8) where an LSA does not provide the requesting CSA with the ‘requested information’.⁴⁹

In the meantime, the Board has dealt with the two requests to order corrective measures within an urgent binding decision following the adoption of provisional measures under Article 61(8). Since the Board was working on guidance on mutual assistance under Article 61 and had not

⁴¹ EDPB 2023A, para. 254.

⁴² Case C-645/19, *Facebook Ireland* (AG Opinion), para. 114.

⁴³ Ibid, para. 116. The alternative approach relying on a request for an EDPB opinion under Art. 64(2) is discussed at paras. 120-121.

⁴⁴ Ibid, para. 117.

⁴⁵ Ibid, para. 119.

⁴⁶ See the commentary on Art. 60 in the first edition of this Commentary at page 969.

⁴⁷ Case C-645/19, *Facebook Ireland* (AG Opinion), para. 119.

⁴⁸ Docksey 2024, p. 244.

⁴⁹ Case C-645/19, *Facebook Ireland*, para. 71.

yet decided its position,⁵⁰ it left open the question of the scope of the obligations under Article 61 and concentrated on the need to fulfil the ‘procedural and substantive criteria’⁵¹ derived from Article 61:

The list provided by Article 61(1) GDPR is not exhaustive (‘in particular’). As such, it does not list or exclude specifically the imposition of corrective measures ... this does not, in any event, remove the duty of the Requested SA, pursuant to Article 61 (4) and 61 (5) GDPR and the general duty of cooperation, to provide reasons for any refusal to comply with a request.⁵²

Applying this approach, the request for corrective measures was rejected in the first urgent binding decision, requested by the Hamburg DPA. The Board found, in part, that the presumption of urgency under Article 61(8) was not applicable, for the procedural reason that the DPA had not used the formal mutual assistance procedure to make its request.⁵³ In contrast, the request for corrective measures was accepted in the second urgent binding decision, requested by the Norwegian DPA, because, in part, the presumption of urgency under Article 61(8) was considered to apply: the local DPA had submitted a request for formal mutual assistance under Article 61 and the LSA had failed to address that request within the timeframe laid down therein.⁵⁴

For future cases, the broad approach to the scope of Article 61 favoured by Advocate General Bobek and the Norwegian and German DPAs would seem to be more in line with the application of the classic interpretation tools used by the CJEU. The Court will interpret a provision in light of its wording, its context and the objectives and purpose pursued by the act of which it forms part, and will prefer an interpretation which ensures that the provision retains its effectiveness.⁵⁵

Considering first the *wording* of Article 61(1), it is not limited to requests for information but defines mutual assistance to cover, ‘in particular’ both ‘information requests’ and ‘supervisory measures.’ Article 61(5) adds that the requested DPA should provide information on ‘the results or, as the case may be, the progress of the measures taken in order to respond to the request.’

As noted above, the specific reference in Article 55(2) of the Commission Proposal, now Article 61(2) GDPR, to ‘enforcement measures to bring about the cessation or prohibition of processing operations contrary to this Regulation’ was removed during the Trilogue. However, the mere removal of this phrase from a non-exhaustive list of measures that a requested authority might take in a separate paragraph of Article 61 does not necessarily affect the scope of Article 61(1), especially since no prohibitive wording was included in the first or second paragraphs of Article 61 to specify that such measures could *not* be requested of, or might *not* be taken by, a requested authority.

⁵⁰ Work Programme 2021-2022 and Work Programme 2023-2024, Pillar II, Supporting effective enforcement and efficient cooperation between national supervisory authorities, at page 3 of each Work Programme, and Work Programme 2024-2025, Pillar 2, Reinforcing a common enforcement culture and effective cooperation, Key Action 1, Encourage and facilitate the use of the full range of cooperation tools enshrined in Chapter VII of the GDPR and Chapter VII of the LED.

⁵¹ EDPB 2023A, paras. 241-243.

⁵² Ibid, para. 244.

⁵³ EDPB 2021, paras. 177-181. See also EDPB 2023A, para. 228.

⁵⁴ EDPB 2023A, paras. 255-257.

⁵⁵ Case C-154/21, *Österreichische Post*, para. 29 and the case-law cited.

Second, the *context* provides some insight into the meaning of a ‘measure’ in Article 61 and recital 133. Article 66 provides that ‘provisional measures’ may be adopted in exceptional circumstances by a DPA, which may then request the Board urgently to adopt ‘final measures.’ Whilst the Board is not obliged to adopt the same measures as the DPA,⁵⁶ there is no doubt that it may adopt corrective measures, which suggests that the concept of ‘measure’ in Chapter VII GDPR may be interpreted consistently as encompassing corrective measures, especially where such action is necessary to ensure compliance with the fundamental right enshrined in Article 8(1) of the Charter.⁵⁷

A similarly broad approach to the scope of mutual assistance can be seen in contemporaneously adopted texts. Article 61 EUDPR requires the EDPS to cooperate with national supervisory authorities ‘to the extent necessary for the performance of their respective duties, in particular by providing each other with relevant information, *asking each other to exercise their powers* and responding to each other’s requests’. Article 13 of Convention 108+ extends the scope of mutual assistance from requests for ‘factual information’ in Convention 108 to ‘coordinating ... investigations or *interventions*’ (emphasis supplied).

Third, the *objective* of ensuring a consistent and high level of protection of natural persons may be found in recital 10 GDPR and the consistent case law of the Court.⁵⁸ In *Facebook Ireland*, AG Bobek pointed out that the Court would not ‘turn a blind eye to any gap ... in the protection of fundamental rights guaranteed by the Charter and their effective enforcement by the competent regulators’,⁵⁹ and the Court itself has subsequently refused to follow an interpretation which would ‘undermine the effectiveness of the protection laid down by that regulation since it would result in persons ... being deprived of protection.’⁶⁰

In this respect, the effectiveness of Article 61 would be reduced if mutual assistance requests by CSAs were limited to requests for information. Provisional measures adopted by CSAs to protect their own citizens under Article 66 may only last three months, and in the event of a refusal by the LSA to extend that protection urgently to individuals across the EEA, they would be unable to benefit from the presumption of urgency specifically envisaged by Article 61(8).

Finally, if an ‘over-eager’⁶¹ DPA continuously resorts to Article 61 without good reason, this should also be considered by the EDPB.

4. Relevant information

The term ‘relevant information’ in Article 61(1) also figures in Article 60(1). It leaves open what information may be considered as ‘relevant’ and thus allows a certain flexibility, to encompass all conceivable elements of the information.

Research has shown that the practice of DPAs was to determine relevancy through contextual criteria, ranging from ‘all pieces of information that are useful in assessing the issue at hand’, to the information needed to ‘take the appropriate procedural and material measures in order

⁵⁶ See section 2.1.3 of the commentary on Art. 66 in this edition.

⁵⁷ Joined Cases T-70/23, T-84/23 and T-111/23, *DPC v EDPB*, para. 56.

⁵⁸ Case C-184/20, *OT v VTEK*, para. 61.

⁵⁹ Case C-645/19, *Facebook Ireland* (AG Opinion), para. 128.

⁶⁰ Case C-46/23, *Újpesti Polgármesteri Hivatal*, para. 45.

⁶¹ Papakonstantinou 2023, pp. 918 and 920.

to solve a case’, and ‘the information which we consider as necessary for adoption of a decision’.⁶²

The EDPB has characterised relevant information in the context of Article 60 as ‘all information that is directly or indirectly conducive to the conclusion of the proceeding’, including ‘sufficient information about the factual elements and legal issues specific to the case’.⁶³ In essence it is the information each DPA needs in order to deal with the case itself.⁶⁴

The EDPB has stressed, with regard to the data minimisation principle in Article 5(1)(c) GDPR, that it should be assessed case by case whether the communication of personal data is necessary.⁶⁵

5. Exchange of information and languages

The GDPR requires relevant information to be provided but does not directly address the question of languages and translations, which inevitably arise in a cross-border and multicultural jurisdiction like the EU. This question was not regulated in the GDPR, as in principle all official EU languages are equal. In practice however information provided between authorities, including accounts on the results of measures, will normally be in English, the common working language of DPAs in cross-border cases,⁶⁶ and the official working language of the Board.⁶⁷ However, it remains possible for two DPAs to agree to use another language. For example, German would be used in a situation involving only German and Austrian DPAs. Moreover the IMI system incorporates an automatic translation tool of text entered into the various fields. In addition, where translations of documents are required in a particular case, DPAs may use the EU institutions’ system of automatic translation, ‘eTranslation’.⁶⁸ These measures have reduced the burden of translation, requiring revision, if necessary, rather than translation *ab initio*.

The Commission has included the regulation of the question of languages and translations in Article 6 of the proposed Procedural Regulation.⁶⁹ The Proposal addresses the question of translations of documents in cross-border cases in two ways. Article 6(1) of the Proposal specifically requires the complaint-receiving DPA to translate complaints and the views of complainants into the language of the LSA, and to translate documents from the LSA, which must be provided to the complainant, into the language of the complainant. In contrast Article 6(2) of the Proposal generally entrusts the EDPB to determine translations of relevant and reasoned objections or comments to LSA draft decisions in its Rules of Procedure. The Commission has not provided any explanation for including specific rules on translations in the Proposal, neither in the explanatory memorandum nor in the two reports on the application of the GDPR.

⁶² See Barnard-Wills et al. 2016, pp. 591–592.

⁶³ EDPB 2022, para. 46.

⁶⁴ Ibid, paras. 47–50. The Board requires its information system, the IMI, to be used for the exchange of such information.

⁶⁵ Ibid, para. 51. Within the IMI, documents containing personal data are kept separate from documents that do not contain such data.

⁶⁶ EDPB-EDPS 2023, para. 69.

⁶⁷ EDPB Rules of Procedure, Art. 23(1).

⁶⁸ See European Commission’s Machine Translation system.

⁶⁹ European Commission 2023.

Unsurprisingly the EDPB and the EDPS have advised against both these provisions, on the basis that Article 6(2) is unnecessary, since such matters may already be determined by the Board under Article 70(1) GDPR. Moreover Article 6(1) of the Proposal would disrupt the existing system based on the common use of a single language, which enables the case handler to verify the correctness of the translated document, and would impose the burden solely on complaint-receiving DPAs.⁷⁰ The European Parliament has suggested that a joint ‘cooperation language’ should be defined which all DPAs must accept for incoming and outgoing information, and that in addition each DPA should define one or more languages that it accepts for incoming information from other DPAs.⁷¹ However, the simplest solution proposed by the Council is not to address translations in the legislation at all,⁷² and to rely on the existing system, based on mutual agreement between DPAs.

6. Formal and informal cooperation

At the end of 2023, the EDPB reported to the Commission on the use of mutual assistance over the five and a half years since the GDPR entered into application.⁷³ The Board found that most DPAs (83%) had used the Article 61 formal mutual assistance procedure in the course of carrying out an investigation, triggering 971 formal requests. The Irish DPA made the most formal requests (246), while German DPAs received the most formal requests (516). An earlier report by the Board on the first 18 months of the GDPR⁷⁴ showed that DPAs only triggered 115 formal mutual assistance requests, which represented a take up of less than half of the current rate, adjusted over a comparable period. The Commission has concluded that DPAs ‘have demonstrated increased willingness to make use of the tools for cooperation provided by the GDPR.’⁷⁵

While requests for formal mutual cooperation under Article 61 have become a significant cooperation tool among DPAs, this has not precluded the development of informal, pre-existing forms of cooperation on the basis of Article 57(1)(g). This provides that DPAs shall cooperate with, ‘including sharing information and provide mutual assistance to,’ other DPAs. Article 57(1)(g) is supported by recital 138, which explains that, in cases where cooperation is not mandatory under the GDPR, ‘mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism’.

To facilitate the use of mutual assistance on an informal basis, for national cases with a ‘cross-border component’, the IMI system includes informal mutual assistance cases in a ‘voluntary mutual assistance’ field. DPAs decided to introduce this procedure to enable a more flexible mutual assistance, based on their prior practice and the general principle of cooperation between them. The Board has confirmed that requests under the voluntary mutual assistance procedure fall outside the procedural requirements of Article 61.⁷⁶

⁷⁰ EDPB-EDPS 2023, paras. 69-71.

⁷¹ Trilogue table, Art. 2d, incorporating the Parliament’s amendments 13 and 66.

⁷² Trilogue table, Art. 6, where the Council position deletes the text.

⁷³ EDPB 2023B, section 4.1.2, pp. 17-19.

⁷⁴ EDPB 2020, section 1.2, pp. 12-13.

⁷⁵ European Commission 2024, p. 2.

⁷⁶ EDPB 2021, paras. 177-178, EDPB 2023A, para. 228.

The informal procedure is used much more often than the formal one,⁷⁷ in particular to inform another DPA about a received complaint, to discuss and solve legal questions which arise in concrete cases, to provide updates on the state of play of a case, to exchange documents, or to request other kinds of information and assistance. While there is no one month legal deadline nor any strict duty to reply, as under Article 61, in practice DPAs reply to voluntary mutual assistance requests within the same period,⁷⁸ although the IMI system allows them to set different non-binding deadlines to reply to informal mutual assistance requests.

It has been rightly argued that ‘informal cooperation is ... crucial for DPA cooperation’, but corresponding fears that the formal cooperation mechanism under the GDPR ‘risks abolishing the cooperation paths already in existence ... which is something that could ultimately harm DPA effectiveness’⁷⁹ have proved to be unfounded. The EDPB has reported that informal mutual assistance has been used extensively over the five and a half years of the application of the GDPR, during which DPAs launched 12,313 procedures to assist each other on a voluntary basis. The Irish DPA initiated the most informal requests for assistance (4245), followed by German DPAs (2036). The EDPB concluded that the voluntary mutual assistance exchange is frequently used, generally effective, and contributes to the uniform understanding and application of the GDPR across the EEA.⁸⁰

Select Bibliography

International instruments

Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS No. 108.

Convention 108+: Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data 2018, CM/Inf(2018)15-final.

Additional Protocol Convention 108: 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 2001, ETS No. 181.

EU legislation

EUDPR: 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 (Text with EEA relevance), OJ 2018 L 295/39.

GDPR: 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) (Text with EEA relevance), OJ 2016 L 119/1.

Regulation 2016/794: Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ 2016 L 135/53, as amended by Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022, OJ 2022 L 169/1.

⁷⁷ EDPB 2023B, p. 17.

⁷⁸ Ibid, p. 19.

⁷⁹ Barnard-Wills 2017, p. 38.

⁸⁰ EDPB 2023B, section 4.1.2, p. 19.

Decision 2018/743: Implementing Decision (EU) 2018/743 of 16 May 2018 on a pilot project to implement the administrative cooperation provisions set out in Regulation (EU) 2016/679 of the European Parliament and of the Council by means of the Internal Market Information System, OJ L 123.

Academic writings

Barnard-Wills et al. 2016: Barnard-Wills, Pauner Chulvi and de Hert, 'Data Protection Authority Perspectives on the Impact of Data Protection Reform on Cooperation in the EU', 32(4) *Computer Law & Security Review* (2016), 587.

Caruana 2024: Caruana, 'Article 50', in Kosta and Boehm (eds), *The EU Law Enforcement Directive (LED), A Commentary* (OUP 2024), 699.

Docksey 2024: Docksey, 'Data Protection at the Court of Justice of the EU, in Van Alsenoy et al (eds), *Two decades of data protection. What Next? EDPS 20th Anniversary* (Publications Office of the European Union 2024), 255.

Gómez Navarro 2024: Gómez Navarro, 'Article 51' in Kosta and Boehm (eds), *The EU Law Enforcement Directive (LED), A Commentary* (OUP 2024), 711.

Papakonstantinou 2023: Papakonstantinou, 'Art. 61 Mutual assistance', in Spiecker gen. Döhmman et al (eds), *General Data Protection Regulation, Article-by-Article Commentary* (Hart Publishing 2023), 915.

Papers of data protection authorities

ICDPPC 2009: International Conference of Data Protection and Privacy Commissioners, 'Joint Proposal for a Draft of International Standards on the Protection of Privacy with Regard to the Processing of Personal Data' (5 November 2009).

ICDPPC 2017: International Conference of Data Protection and Privacy Commissioners, 'Global Cross Border Enforcement Cooperation Arrangement' v17, Annex One to Resolution on exploring future options for International Enforcement Cooperation (September 2017).

EDPB Rules of Procedure: European Data Protection Board, 'Rules of Procedure' (25 May 2018).

EDPB 2020: European Data Protection Board, 'Contribution of the EDPB to the evaluation of the GDPR under Article 97' (18 February 2020).

EDPB 2021: European Data Protection Board, 'Urgent Binding Decision 01/2021 on the request under Article 66(2) GDPR from the Hamburg (German) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited' (12 July 2021).

EDPB 2022: European Data Protection Board, 'Guidelines 02/2022 on the application of Article 60 GDPR' (14 March 2022).

EDPB 2023A: European Data Protection Board, 'Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR)' (27 October 2023)

EDPB 2023B: European Data Protection Board, 'Contribution of the EDPB to the report on the application of the GDPR under Article 97' (12 December 2023).

EDPB-EDPS 2023: European Data Protection Board and European Data Protection Supervisor, 'Joint Opinion 01/ 2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679' (19 September 2023).

WP29 2011: Article 29 Working Party, 'Advice Paper on the Practical Implementation of the Article 28(6) of the Directive 95/46/EC' (20 April 2011).

WP29 2013: Article 29 Working Party, ‘Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (“DPIA Template”) Prepared by Expert Group 2 of the Commission’s Smart Grid Task Force’ (WP 205, 22 April 2013).

Reports and recommendations

Barnard-Wills and Wright 2015: Barnard-Wills and Wright, ‘Authorities’ Views on the Impact of the Data Protection Framework Reform on their Co-Operation in the EU’, Deliverable D1 for the PHAEDRA II project (20 July 2015).

Barnard-Wills 2017: Barnard-Wills, Papakonstantinou, Pauner Chulvi and Díaz Lafuente, ‘Recommendations for Improving Practical Cooperation between European Data Protection Authorities’, Deliverable D4.1 for the PHAEDRA II project (14 January 2017).

ChatGPT Taskforce Report: European Data Protection Board, ‘Report of the work undertaken by the ChatGPT Taskforce’ (23 May 2024).

Cookie Banner Taskforce Report: European Data Protection Board, ‘Report of the work undertaken by the Cookie Banner Taskforce’ (17 January 2023).

European Commission 2023: European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679’, COM(2023) 348 final, 4 July 2023.

European Commission 2024: European Commission, ‘Second report on the application of the General Data Protection Regulation (GDPR)’, COM(2024) 357 final, 25 July 2024.

OECD Recommendation 2007: Organisation for Economic Co-operation and Development, ‘Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy’, 2007.

Papakonstantinou 2016: Papakonstantinou, Pauner Chulvi, Cuella and Barnard-Wills, ‘European and National Legal Challenges when Applying the New General Data Protection Regulation Provisions on Co-Operation’, Deliverable D3.1 for the PHAEDRA II project (15 September 2016).

Supervisory Authorities Report: European Data Protection Board, ‘Report of the work undertaken by the supervisory authorities within the 101 Task Force’ (28 March 2023).

Trilogue table: General Secretariat of the Council, Interinstitutional File 2023/0202(COD), document 1510/24, four-column table concerning the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, which contains the Commission proposal of 4 July 2023, the amendments adopted by the European Parliament on 10 April 2024, and the Council’s mandate approved on 13 June 2024.

Others

EDPB Subgroups & Taskforces: European Data Protection Board, ‘EDPB plenaries, subgroups and taskforces’, available at https://www.edpb.europa.eu/about-edpb/who-we-are/edpb-plenaries-subgroups-and-taskforces_en.

European Commission’s Machine Translation system: European Commission, ‘eTranslation’, available at https://commission.europa.eu/resources-partners/etranslation_en.

GPEN Website: Global Privacy Enforcement Network, ‘Website’, available at <https://www.privacyenforcement.net/>.

Work Programme 2021/2022: European Data Protection Board, ‘EDPB Work Programme 2021/2022’, available at https://www.edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf.

Work Programme 2023/2024: European Data Protection Board, ‘EDPB Work Programme 2023/2024’, available at https://www.edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-work-programme-2023-2024_en.

Work Programme 2024/2025: European Data Protection Board, ‘EDPB Work Programme 2024/2025’, available at https://www.edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-work-programme-2024-2025_en.

Article 89. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

*LAURA DRECHSLER AND CHARLOTTE SOMERS**

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.
2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.
3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.
4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Relevant Recitals

(156) The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and

* This contribution is based on the first edition of the Commentary in which Christian Wiese Svanberg authored the contribution on Art. 89.

derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

(157) By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.

(158) Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes.

(159) Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.

(160) Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

(161) For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No. 536/2014 of the European Parliament and of the Council should apply.

(162) Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality. Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.

(163) The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU, while national statistics should also comply with Member State law. Regulation (EC) No. 223/2009 of the European Parliament and of the Council provides further specifications on statistical confidentiality for European statistics.

CLOSELY RELATED PROVISIONS

Article 4 (Definitions) (see too recital 26); Article 5 (Principles relating to processing of personal data); Article 6 (Lawfulness of processing) (see too recital 50); Article 9 (Processing of special categories of personal data) (see too recitals 52–53)

RELEVANT CASE LAW

CJEU

Case C-524/06, *Heinz Huber v Bundesrepublik Deutschland*, judgment of 16 December 2008 (Grand Chamber) (ECLI:EU:C:2008:724).

Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, judgment of 13 May 2014 (Grand Chamber) (ECLI:EU:C:2014:317).

Opinion of Advocate General Jääskinen in C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, delivered on 25 June 2013 (ECLI:EU:C:2013:424).

Case C-507/17, *Google LLC, venant aux droits de Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, judgment of 24 September 2019 (Grand Chamber) (ECLI:EU:C:2019:772) ('Google v CNIL').

Case C-136/17, *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)*, judgment of 24 September 2019 (Grand Chamber) (ECLI:EU:C:2019:773).

ECtHR

Von Hannover v Germany (No. 2), Appl. Nos. 40660/08 and 60641/08, judgment of 7 February 2012 (Grand Chamber).

Axel Springer v Germany, Appl. No. 39954/08, judgment of 7 February 2012 (Grand Chamber).

M.L. and W.W. v Germany, Appl. Nos. 60798/10 and 65599/10, judgment of 28 June 2018.

Hurbain v Belgium, Appl. No. 57292/16, judgment of 4 July 2023 (Grand Chamber).

Austria

Austrian Federal Administrative Court (*Bundesverwaltungsgericht*), judgment of 17 May 2022, W256 2225038-1.

Belgium

Belgian Court of Appeal Brussels (*Hof van beroep Brussel*), judgment 2024/AR/121 of 11 December 2024.

Germany

German Federal Constitutional Court (*Bundesverfassungsgericht*), judgment 1 BvR 209, 269, 362, 420, 440, 484/83 of 15 December 1983 ('*Volkszählungsurteil*').

German Administrative Court Hamburg (*Verwaltungsgericht Hamburg*), judgment of 28 July 2022 (ECLI:DE:VGHH:2022:0728.21K1802.21.00).

Netherlands

Dutch Supreme Court (*Hoge Raad*), judgment of 21 July 2023 (ECLI:NL:PHR:2023:823).

A. Rationale and Policy Underpinnings

As is the case with the other provisions of Chapter IX, Article 89 GDPR enumerates specific processing situations in regard to which the EU legislator has deemed it necessary to allow the processing of personal data, subject to appropriate safeguards. For Article 89, these interests are threefold: (1) archiving purposes in the public interest; (2) scientific and research purposes; and (3) statistical purposes.¹

The fundamental reason for providing what is in practice a broad margin for Member States to accommodate these purposes is the recognition of their important role in society,² and the fact that they cannot be accomplished without the processing of personal data.³ In practice, this means that the fundamental question from a data protection standpoint is often not whether processing may take place, but rather how it can take place — i.e. which safeguards are needed to keep an appropriate balance between the various general purposes covered by Article 89 and the protection of fundamental rights and freedoms of individuals.⁴

B. Legal Background

1. EU legislation

The DPD recognised the fundamental interests enumerated in Article 89 with regards to data processing for historical, statistical or scientific purposes and allowed Member States to deviate from certain key principles to that end, provided that there were 'suitable safeguards'.⁵ Yet, the DPD provided little detail on how such suitable safeguards should be designed. It only mentioned that they were supposed to 'rule out the use of the data in support of measures or decisions regarding any particular individual'.⁶ In practice, the framework of the DPD allowed

¹ Art. 89(1) GDPR.

² E.g. research is a key objective of the EU as set out in Art. 179 TFEU.

³ For research, this has been recognised from the beginning of regulatory efforts in Europe. See Simitis 1981.

⁴ Carmichael, Craddock and Stalla-Bourdillon 2023, p. 1115.

⁵ See rec. 29 and 40, and Art. 6(1)(b) and (e) DPD. See further Pormeister 2017.

⁶ Rec. 29 DPD.

for national legislation with a scope similar to that now mandated under Article 89, even though there was no fully equivalent provision.

The addition of a regime for ‘archiving purposes in the public interest’ is one of the innovations of the GDPR. This does not necessarily mean that archiving purposes were not granted any exception under the DPD. They might have partly overlapped with the purpose of ‘historical research’, which was explicitly mentioned.⁷

2. International instruments

Both Convention 108 and Convention 108+ foresee possibilities for Member States to impose restrictions on certain individual rights for purposes safeguarded in Article 89 GDPR. Convention 108 includes this possibility for ‘automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects’.⁸ Convention 108+ extends this list to ‘archiving purposes in the public interest, scientific or historical research purposes or statistical purposes’.⁹

Like the GDPR, Convention 108+ therefore explicitly adds archiving in the public interest as a privileged purpose.¹⁰ This development should also be seen against the recommendation of the Council of Europe from 2000 regarding the accessibility of archives which points out the need to balance data protection requirements with a general policy of public access to archives.¹¹ A recent study on the implementation of this recommendation in all Member States of the Council of Europe confirmed that this balance remains a challenge.¹²

In addition, the Council of Europe has issued recommendations in the domain of health-related data and biological materials of human origin which aim to safeguard fundamental rights of the persons whose biological materials are intended for biomedical research.¹³ These recommendations set conditions for the use of biological materials in research projects when consent from the individual concerned cannot be obtained.¹⁴

Research as a privileged purpose is especially relevant in the context of Artificial Intelligence (AI) and has therefore been given special consideration in regulatory initiatives concerning AI. For example, the Council of Europe’s Framework Convention on AI stipulates that it does not apply to research and development activities related to AI systems that are ‘still in the experimental or pre-commercial phase’, unless the testing or other activities are undertaken in such a way that they could potentially interfere with human rights, democracy and the rule of law.¹⁵

⁷ See further Carmichael, Craddock and Stalla-Bourdillon 2023, p. 1117.

⁸ Art. 9(3) Convention 108.

⁹ Arts. 8(3), 9(2) and 11 Convention 108+.

¹⁰ See further the introduction of a compatibility presumption in *ibid.*, Art. 5(4)(b).

¹¹ Committee of Ministers of the Council of Europe 2000.

¹² Friedewald, Székely and Karaboga 2024, pp. 36 and 61.

¹³ Council of Europe 2016.

¹⁴ *Ibid.*, Art. 21.

¹⁵ Art. 3(3), AI Framework Convention.

3. National developments

Member States have taken different approaches in implementing Article 89 GDPR in their national legislation.¹⁶ While some rely directly on or merely reference Article 89 GDPR without offering further clarification,¹⁷ others regulate these safeguards in great detail, sometimes through specific laws dedicated to research and data protection.¹⁸

Overall, the types of safeguards employed are broadly similar across the Member States. Common measures include anonymisation, pseudonymisation as part of data minimisation efforts, and technical and organisational safeguards like access controls, appointing responsible individuals for research oversight, and security management protocols.¹⁹ There are also specific provisions for the handling of special categories of personal data which serve as important converging safeguards across the Member States.²⁰ However, significant differences exist in the more detailed requirements which can affect the level of protection provided. These include variations in how the concept of scientific research is interpreted, differing emphasis on the importance of public interest, and varying consent requirements.²¹ As a result, while the general approach seems consistent across the EU Member States, the specifics of these safeguards vary considerably in both their detail and the level of protection they offer.

4. Case law

The CJEU has not dealt so far with a case directly involving the interpretation of Article 89 GDPR. It has issued relevant case law to understand the balancing underlying Article 89 and the finding of appropriate safeguards to achieve such a balance. Moreover, for all purposes covered by Article 89 GDPR, the CJEU's case law on the 'right to be forgotten' is relevant as it discusses the balancing of the fundamental rights of privacy and personal data protection with the freedom of information as part of the right to freedom of expression.²² All three purposes of Article 89 GDPR (research, archiving and statistics) can arguably be linked to the wider protective realm of freedom of information.²³ The most comprehensive cases in this regard are two decisions taken by the CJEU's Grand Chamber in 2019 on de-listing.²⁴ Both cases recognize the right of the public to access information as a consideration influencing the balancing.²⁵ This is a change from the previous decision of the CJEU in *Google Spain* where this interest was not as explicitly highlighted.²⁶ However, both cases also make clear that this right is in principle outweighed by an individual's right to privacy and personal data protection, unless there are substantial reasons justifying the public interest in the information — i.e. strict

¹⁶ See e.g. Timmers et al. 2018; Kindt et al. 2021.

¹⁷ See e.g. Bulgarian Personal Data Protection Act, Art. 25n; Polish Personal Data Protection Act.

¹⁸ See e.g. Austrian Federal Data Protection Act, §7 and Austrian Research Organisation Act; Arts. 132-137 and 197-208 Belgian GDPR Implementation Law; Arts. 4 and 78 French Data Protection Act 1978 and Art. 116 French implementing decree; Art. 27 German Federal Data Protection Act 2017.

¹⁹ Kindt et al. 2021.

²⁰ See e.g. Arts. 44 and 65 French GDPR Implementation Law.

²¹ Kindt et al. 2021.

²² See further the commentary on Art. 17 in this edition.

²³ Woods 2021.

²⁴ Case C-507/17, *Google v CNIL*; Case C-136/17, *GC and Others*.

²⁵ Case C-507/17, *Google v CNIL*, para. 45; Case C-136/17, *GC and Others*, para. 66. See further Pollicino 2021, p. 81.

²⁶ Compare to Case C-131/12, *Google Spain*, para. 99.

necessity for freedom of expression.²⁷ The CJEU highlights ‘the role played by the data subject in public life’ as a key consideration of the balancing.²⁸

The balancing of freedom of information as part of freedom of expression with privacy has a long history in the case law of the European Court of Human Rights (‘ECtHR’),²⁹ to which the CJEU explicitly refers.³⁰ Especially noteworthy is a recent Grand Chamber judgment concerning the balancing of freedom of information with privacy in the context of newspaper archiving.³¹ While previous decisions of the ECtHR highlighted the importance of newspaper archives and thus denied a need to allow for erasure requests,³² in *Hurbain v Belgium* the ECtHR turned a new leaf and recognized that there might be cases where individual interests outweighed the need for having the content of news in a publicly accessible archive.³³

In the area of statistical purposes, the *Huber* judgment is the leading case.³⁴ It concerned an Austrian resident in Germany who requested the deletion of personal data relating to him in the German Central Register of Foreign Nationals. The register was used for statistical purposes and by security and police services and judicial authorities for the prosecution and investigation of criminal activities. The Court held that only the processing of anonymous information was required in order for the statistical objectives of the database to be attained, so that it could not be said that the processing of personal data in this case was ‘necessary’, suggesting a strict interpretation of necessity when it comes to the privileges in data protection law for statistical purposes.³⁵

Article 89 GDPR plays a more dominant role in national case law and decisions of data protection authorities of the different Member States. A systematic research of case law on GDPR Hub revealed a handful of decisions on all three purposes. Most cases concern the key question whether sufficient appropriate safeguards were implemented in order to benefit from the privileges the GDPR foresees for processing operations for research, archiving in the public interest, and statistics.³⁶

²⁷ Case C-507/17, *Google v CNIL*, para. 45; Case C-136/17, *GC and Others*, para. 66.

²⁸ Case C-507/17, *Google v CNIL*, para. 66.

²⁹ See e.g. ECtHR, *Von Hannover v Germany*; ECtHR, *Axel Springer v Germany*.

³⁰ See e.g. Case C-507/17, *Google v CNIL*, para. 76; Case C-131/12, *Google Spain* (AG Opinion), para. 123.

³¹ ECtHR, *Hurbain v Belgium*.

³² See e.g. ECtHR, *M.L. and W.W. v Germany*, para. 90.

³³ ECtHR, *Hurbain v Belgium*, para. 255.

³⁴ Case C-524/06, *Huber*.

³⁵ *Ibid.*, para. 65. For a discussion of a potentially broader interpretation of ‘necessity’, see para. 62, where the CJEU argues that centralisation of data may be necessary if it leads to a more effective application of the law. See the commentary on Art. 6 in the first edition of this Commentary at page 336 for an interpretation of ‘necessity’ in *Huber* in the context of Art. 6(1)(e) GDPR.

³⁶ See e.g. for research: Italian DPA 2024; French DPA 2023; Austrian DPA 2023, Spanish DPA 2021. For archiving in the public interest: Norwegian Privacy Appeals Board 2023; Bundesverwaltungsgericht, judgment of 17 May 2022; Hoge Raad, judgment of 21 July 2023. For statistics: Verwaltungsgericht Hamburg, judgment of 28 July 2022; Italian DPA 2023; Portuguese DPA 2022; Norwegian DPA 2023.

C. Analysis

1. Introduction

The interaction between data protection law, archiving in the public interest, research and statistics has been complex.³⁷ Especially for research, arguments have been made that the GDPR poses an obstacle to effective research, particularly health research, and these arguments became prevalent during the Covid-19 crisis.³⁸ To a lesser extent, the GDPR has also been identified as an obstacle for archiving, as it might lead to conflicts between the public's interest in preserving information and an individual's control over their own information online.³⁹ Processing of personal data for statistical purposes led to the famous *Volkszählungsurteil* of the German Constitutional Court,⁴⁰ establishing the right to informational self-determination, which some argue still lies at the core of EU data protection law.⁴¹

Article 89 is meant to achieve an appropriate balance between the different interests at stake in all three areas. It is addressed both to parties that conduct archiving, research and statistical processing, and to the EU and Member State legislators (with regard to the enactment of derogations). It is important to note that Article 89 does not by itself provide a legal basis for data processing. It operates on the basis of a number of key provisions of the GDPR referring to it, as is further discussed in section 3 below. Taken together with these key provisions, Article 89 provides the framework for the privileged position of processing for the purposes of research, archiving in the public interest, and statistics. Nevertheless, two inherent characteristics of Article 89 challenge this presumed privilege: (1) the lack of detail when it comes to the 'appropriate safeguards' that are needed for benefitting from the privilege; and (2) the fact the privilege depends on Member State law to be fully effective, which in turn results in a fragmented landscape for the privileged purposes.

Infringements of Article 89 are subject to the higher level of administrative fines under Article 83(5)(c), i.e. up to € 20 million or 4 per cent of the total worldwide turnover of the preceding financial year, whichever is higher.

2. The three purposes of Article 89 GDPR

Article 89 GDPR regulates three distinct and separate purposes: archiving in the public interest, scientific or historical research purposes and statistical purposes. Common to all three purposes is that the formal definition of the individual purpose is largely left to the discretion of the Member States. Similarly, the extent to which the pursuit of one of these purposes can be a task delegated wholly or partly to private entities is left to Member States to determine. This means that, in practice, the detailed requirements for the types of data processing described in Article 89 are determined under Member State law.

³⁷ For discussion of the issues in the context of research, see Simitis 1981; Forgó 2015; Pormeister 2017; Rumbold and Pierscionek 2017; Timmers et al. 2018; Comandé and Schneider 2022. For archiving, see National Archives 2018; Friedewald, Székely and Karaboga 2024. For statistics, see Bundesverfassungsgericht, *Volkszählungsurteil*.

³⁸ See e.g. ALLEA et al. 2021.

³⁹ See e.g. Ctvrtník 2023; Hafner 2024.

⁴⁰ Bundesverfassungsgericht, *Volkszählungsurteil*.

⁴¹ Rouvroy and Poulet 2009.

2.1 Archiving in the public interest

Article 89(3) GDPR permits derogations for ‘archiving in the public interest’. According to recital 158, services covered by this definition include ones ‘which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest’.⁴² This suggests that not every archiving activity will fall under the scope of Article 89, but only those that are covered by a legal obligation to maintain records as described above. Certain archives such as personal or family archives or company records are therefore only covered by Article 89 if they fulfil the criteria of being kept in the ‘public interest’ and ideally have a legal obligation backing up their claim.

The requirement that archiving must take place ‘in the public interest’ should be regarded as satisfied as long as any individual archiving activity is set out — even broadly — in Member State law. Thus, the GDPR does not limit the extent to which Member States can delimit what materials are of sufficient historical interest to warrant subjecting them to archiving rules. Case law from the ECtHR suggests that news archives fall under an archiving activity for the public interest due to their relevance for freedom of expression, without necessarily requiring a legal basis in Member State law.⁴³ For other archiving activities, the discussion remains ongoing.

An interesting case study is the discussion on baptism registries kept by the Catholic church. Requests for erasure from these registries have led to court or DPA decisions in both Slovenia and Belgium with opposite outcomes. As reported to the EDPB by the Slovenian DPA, in Slovenia, the DPA and then the court, found a clear obligation in the Slovenian law to keep records related to baptisms and thus applied the regime of Article 89 fully (in particular the derogation based on it for the right to erasure).⁴⁴ In Belgium, the DPA could not find such a legal basis and also considered that the main objective of these registries was not to preserve the data for archiving or research purposes, thus the privileged regime of Article 89 did not apply, and erasure would have to be allowed.⁴⁵ The decision is currently undergoing an appeal before a Belgian court, which in turn has led to questions being sent to the CJEU.⁴⁶ The reference has the potential to provide far-reaching insights into the role of archiving in the public interest for the system of the GDPR and the privileges of Article 89.

Another open question relating to processing for archiving in the public interest is how to handle data relating to deceased persons. The GDPR provides in its recitals that it should not apply to deceased persons.⁴⁷ Many of the archives to which Article 89 applies will necessarily contain the data of such persons and thus (some) processing activities appear out of scope of the GDPR (especially those relating to a period more than a normal human life-time ago).⁴⁸ However, Member States may provide for rules regarding the processing of personal data of the deceased,⁴⁹ and they are also authorised to provide for the further processing of personal data in archives that include ‘specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the

⁴² Rec. 158 GDPR. See further EAG Guidelines 2018.

⁴³ ECtHR, *Hurbain v Belgium*, para. 180.

⁴⁴ EDPB News 2021.

⁴⁵ Belgian DPA 2023.

⁴⁶ Hof van beroep Brussel, judgment 2024/AR/121 of 11 December 2024.

⁴⁷ See rec. 27, 158 and 160 GDPR.

⁴⁸ EAG Guidelines 2018; Ctvrtník 2023.

⁴⁹ Rec. 27 GDPR.

Holocaust, or war crimes’,⁵⁰ which would seem to consist in significant part of persons who are deceased. Thus, the processing of personal data of the deceased is a matter left to national law and to European human rights law.⁵¹ With regard to archiving under the GDPR, the best view seems to be that, while archives solely containing the personal data of deceased persons are not subject to the GDPR, archives are not removed from the rules of Article 89 (and the GDPR in general) just because they contain some data of deceased persons. In other words, most archives will be in scope as their information contains both data on living and deceased persons.⁵² Moreover, Member State law may also be relevant in such cases.

In some cases, it can also not be excluded that personal data relating to a deceased person is also personal data on a living person.⁵³ For example, if the archived information reveals rare genetic diseases then it would still constitute health data of any descendants. An open question is whether archived information revealing sensitive matters of a family’s history, such as their role during WWII, should be considered as personal data of the descendants, especially if it is easily findable online based on a name-search.⁵⁴

The GDPR does not require that archiving be carried out in a particular manner. Thus, it may be centralised with one or more state-owned or private bodies, make use of private sector entities and encompass flexible arrangements whereby relevant materials are archived locally with the entity which originally produced them, as long as such a practice is governed by relevant and sufficiently detailed legislation and subject to appropriate safeguards as required in Article 89.⁵⁵

2.2. Scientific or historical research purposes

Recital 157 emphasises the critical role that registries play in advancing scientific research. Coupling information from registries can provide researchers with new insights and enhance the reliability and scope of research by offering data from larger populations, which strengthens the quality of research outcomes. The recital underscores that such high-quality knowledge can inform better policy-making and enhance the efficiency of social services. While no explicit definition of ‘registries’ is given, the recital suggests that registries refer to organised collections of personal data, often created for specific purposes such as scientific research, health monitoring, or social studies. The interpretation of registries as structured data repositories can also be found in national legislation.⁵⁶ Recital 159 states that ‘the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research’.

⁵⁰ Rec. 158 GDPR.

⁵¹ Erdos 2021; Harbinja 2023.

⁵² Ctvrtník 2023.

⁵³ Erdos 2021, p. 21.

⁵⁴ This is currently discussed in the Netherlands, due to a planned public release of a large number of documents linked to WWII. See Consortium Oorlog voor de Rechter 2024.

⁵⁵ A study in 2024 on the CoE Recommendation on archiving of 2000 reveals that most archives work with a system where data are stored for a certain period before being transferred to a national archive. For appropriate safeguards most archives work with blocking periods for data that are personal and/or sensitive. The report identifies 30 years for personal data and up to 100 years for sensitive data as the norm. See Friedewald, Székely and Karaboga 2024.

⁵⁶ See e.g. the German Federal Cancer Registry Data Act.

The recitals provide a broad enumeration of the types of scientific research that can be carried out under Article 89, including as examples medical research into cardiovascular disease, cancer and depression, and registry-based research whereby information from registries is coupled to enable researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions.⁵⁷ The term also includes studies conducted in the public interest in the area of public health.⁵⁸ In conclusion, the GDPR adopts a wide concept of research, covering many types of research, including those in the ‘hard sciences’, social sciences etc.⁵⁹

On 2 February 2021, the EDPB released a document to address misunderstandings and misinterpretations regarding the application of the GDPR to scientific health research.⁶⁰ This document, issued under Article 70(1)(b) GDPR, responds to questions from the European Commission and discusses necessary safeguards that should be put in place in the context of scientific health research under Article 89(1). Although the document briefly touches on key issues, such as the anonymisation and pseudonymisation of health data, it indicates that these topics will be explored in greater detail in forthcoming guidelines. These guidelines on the processing of personal data for scientific research purposes were expected by the end of 2021 but have not yet been published.

The exact meaning of historical research is not set out. However, the term encompasses both historical research and research for genealogical purposes.⁶¹ As discussed above with regard to archiving in the public interest, the GDPR does not apply to deceased persons in the context of scientific or historical research purposes as well.⁶² However, Article 89 remains relevant when such processing involves data related to deceased persons. Additionally, Member States have the discretion to enact legislation concerning the data of deceased individuals, leading to a variety of approaches across Europe.⁶³

Parties involved in scientific research, particularly in the health context, should be prepared to implement further protections if they are in the interest of the data subject, and to apply the general rules of the GDPR with regard to such further protections.⁶⁴ Regarding the question on how the result of scientific research may be disseminated to the public via publication, and thus ensure the public value of the research is realised, Member States are required to ensure specific conditions apply ‘in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes’.⁶⁵

In April 2020, the EDPB issued guidelines on the processing of health data for scientific research in the context of the COVID-19 pandemic.⁶⁶ These guidelines provide insight into how Member States may establish specific GDPR derogations for scientific research under Article 89(2). They also outline the appropriate safeguards required under Article 89(1) to

⁵⁷ Rec. 157 GDPR.

⁵⁸ Rec. 159 GDPR.

⁵⁹ *Ibid.*; EDPS 2020, 11-12.

⁶⁰ EDPB 2021.

⁶¹ Rec. 160 GDPR.

⁶² *Ibid.*

⁶³ See e.g. Art. 3 Spanish Data Protection Act 2018. See for research on post-mortem privacy and how different jurisdictions address these matters concerning data of deceased individuals: Edwards and Harbinja 2013, Erdos 2021 and Harbinja 2023.

⁶⁴ Rec. 159 GDPR.

⁶⁵ *Ibid.*

⁶⁶ EDPB 2020A.

ensure that personal data are adequately protected during such research activities. Furthermore, a study by the European Commission from February 2021 describes and assesses Member States' domestic rules on the processing of health data in light of the GDPR.⁶⁷ The study suggests that most Member States have made use of the opening clause in Article 89(2) to adopt sectoral rules on the processing of health data for scientific purposes, leading to considerable fragmentation in the way health data processing is regulated across the EU.

The GDPR as a whole, and Article 89 in particular, do not distinguish between scientific research pursuing public interests and that pursuing private or purely commercial research.⁶⁸ Therefore, scientific research can be conducted not only by academic researchers but also by non-profit organisations, government institutions, and profit-driven commercial companies.⁶⁹ As long as the requirements of the GDPR and applicable Member State law are met, purely private or commercial interests can be pursued through the processing of personal data for scientific research purposes. Any other relevant legislation (such as legislation on clinical trials in the case of medical or scientific research) will also continue to apply.⁷⁰ Furthermore, if the result of scientific research gives reason for further measures in order to protect the interests of data subjects, then the general rules of the GDPR will apply to such further measures.⁷¹

Consent can be the legal basis for conducting research in accordance with the GDPR.⁷² If it is not possible to fully identify the purpose of the data processing for the scientific research purposes at the time of data collection, the data subjects can give their consent to certain areas of scientific research or parts of research projects to the extent allowed by the intended purpose.⁷³ However, other lawful bases may apply with regard to processing data for research purposes, as long as appropriate safeguards are in place.⁷⁴

Data protection within research projects is not only regarded as a legal requirement but is also considered an ethical requirement, meaning that compliance with the GDPR is viewed as part of ethical standards researchers must meet.⁷⁵ Moreover, Data Management Plans (DMPs) are considered as a best practice for ensuring compliance with research data protection regulations. For instance, national funding bodies are increasingly requiring researchers to submit DMPs as part of their funding applications or in the initial phases of the project.⁷⁶ The DMP serves as a tool for the researcher during the planning and execution of the research, ensuring that researchers have considered how they will process and protect data to align with both ethical and legal standards for data protection.

⁶⁷ EC Study 2021.

⁶⁸ See Rec. 159 GDPR: 'including for example technological development and demonstration, fundamental research, applied research and privately funded research'. For discussion and definition efforts on the concept of 'scientific research', see Bentzen 2020.

⁶⁹ EDPS 2020, 11.

⁷⁰ Rec. 156 GDPR. See also EDPB 2019.

⁷¹ Rec. 159 GDPR.

⁷² Art. 6(1)(a) and rec. 33 GDPR.

⁷³ Ibid.

⁷⁴ EDPB 2020B.

⁷⁵ See e.g. European Commission 2021. See critically on the conflation of law and ethics: Wagner 2018.

⁷⁶ For instance, beneficiaries of the Horizon Europe Programme must establish a DMP. Likewise, the Research Foundation Flanders (FWO) mandates that a provisional DMP be submitted by the sixth month of the project. See e.g. FWO 2024; Horizon Europe Regulation, Art. 39(4).

2.3. Statistical purposes

Recital 162 defines ‘statistical purposes’ as ‘any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results’. The non-personal nature of aggregate or statistical data means that they are not to be used ‘in support of measures or decisions regarding any particular natural person’.⁷⁷ Union or Member State law must also enact a number of protections for data used for statistical purposes, within the limits of the GDPR. In particular, they should ‘determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality’.⁷⁸ There are also special rules covering information which the EU institutions and national statistical authorities collect for the production of official European and national statistics;⁷⁹ in particular, Article 338(2) TFEU applies to the development, production and dissemination of European statistics,⁸⁰ and national statistics must comply with Member State law. Regulation EC No. 223/2009 also applies with regard to statistical confidentiality for European statistics.⁸¹

3. The general principle of Article 89(1)

Under Article 89(1) GDPR, ‘appropriate safeguards’ must be put in place whenever personal data are processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In particular, the provision requires the use of technical and organisational measures to achieve data minimisation, which is defined in Article 5(1)(c) GDPR as personal data being processed in a way that is ‘adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed’.⁸² Recital 156 mentions anonymisation in this regard, and the reference in Article 89(1) to ‘further processing which does not permit or no longer permits the identification of data subjects’ could be interpreted as including anonymisation. In addition, Article 89(1) specifically mentions pseudonymisation. Thus, anonymisation and pseudonymisation are favoured as safeguards under Article 89, although the list of safeguards mentioned therein is not exhaustive. The generality and limited scope of the safeguards in Article 89(1) have been criticized.⁸³ Case law from the national DPAs and courts reveals that what counts as appropriate safeguards in a given processing context is a frequent point of discussion.⁸⁴ An example of a more detailed discussion is a decision by the CNIL of September 2023, where it assessed the safeguards needed for a longitudinal survey on work-life balance.⁸⁵ The decisions on Article 89 GDPR from the Member States also frequently emphasise the importance of putting in place sound data security measures as part of the required safeguards.⁸⁶

The phrase at the end of Article 89(1), that ‘those purposes *shall* be fulfilled in that manner’ (emphasis added), may seem to require anonymisation or pseudonymisation. However, this

⁷⁷ Rec. 162 GDPR.

⁷⁸ Ibid.

⁷⁹ Rec. 163 GDPR.

⁸⁰ Ibid.

⁸¹ Ibid. See further Regulation 223/2009.

⁸² See the commentary on Art. 5 in this edition.

⁸³ See Pormeister 2017, p. 139; see also criticism and suggestions for possible safeguards for biobank, databank and genetic research in Staunton et al. 2022.

⁸⁴ E.g. Italian DPA 2024; French DPA 2023; Spanish DPA 2021.

⁸⁵ French DPA 2023.

⁸⁶ See e.g. *ibid.*; Verwaltungsgericht Hamburg, judgment of 28 July 2022; Hoge Raad, judgment of 21 July 2023.

will largely depend on which purposes are being pursued. In some areas, such as in medical research, they are widely used. But in others, a requirement to anonymise or pseudonymise personal data that have been deemed worthy of preservation (e.g. that are processed for archiving purposes) may make little sense, as removing the nexus between people and events would negate the purpose of the processing. The fact that anonymisation and pseudonymisation should only be used when this would not defeat the purpose of the processing is emphasised by the wording in Article 89(1) ‘Where those purposes can be fulfilled by further processing . . .’. Furthermore, the border between anonymisation and pseudonymisation is not always easy to establish.⁸⁷ For example, in an Italian case concerning the participation of the city of Trento in several EU research projects, the Italian DPA considered the measures taken as constituting pseudonymisation, whereas the city of Trento had classified them as anonymisation.⁸⁸

The appropriate safeguards required under Article 89(1) are of high importance as the whole privileged regime for archiving in the public interest, research and statistical processing depends on their existence.⁸⁹ The provisions introducing the privileges (see for an overview *Table 1* below) always refer to Article 89(1) GDPR as one of the conditions. In some cases, the privilege will also depend on whether the privileged purpose would be disproportionately affected or seriously impaired if the normal rules are applicable. It is thereby not clear whether this has to be shown for the particular case at hand or if the determination could already be made within the national law specifying Article 89(1). Existing national case law from the DPAs and courts shows that both options exist in the Member States.⁹⁰

Table 1: Privileges in the GDPR for archiving in the public interest, research, and statistical processing⁹¹

Article in the GDPR	Privilege
Article 5(1)(b) (‘purpose limitation’)	‘...further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in compliance with Article 89(1), not be considered to be incompatible with the initial purposes...’
Article 5(1)(e) (‘storage limitation’)	‘... personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject...’
Article 9(2)(j) (‘processing of special categories of personal data’)	‘Paragraph 1 shall not apply if one of the following applies: (...) (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject...’
Article 14(5)(b) (‘Information to be provided where personal data have not been obtained from the data subject’)	‘Paragraphs 1 to 4 shall not apply where and insofar as: (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall

⁸⁷ WP29 2014; AEPD and EPDS 2021.

⁸⁸ Italian DPA 2024.

⁸⁹ Rec. 156 GDPR.

⁹⁰ Individual assessment: Austrian DPA 2021; Norwegian Privacy Appeals Board 2023. Assessment done in the law: EDPB News 2021.

⁹¹ See further the commentaries on Arts. 5, 9, 14, 17 and 21 in this edition.

	take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available...'
Article 17(3)(d) ('Right to erasure ('right to be forgotten'))	'Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: ... (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing...'

4. Restrictions to data subject rights (Articles 89(2), (3) and (4))

Articles 89(2)–(3) provide for derogations from the exercise of certain rights when personal data are processed for the purposes of archiving in the public interest, research, or statistical purposes.⁹² The application of these derogations is conditioned on the protections of the appropriate safeguards of Article 89(1) and Union or Member State law. Thus, appropriate safeguards must be in place to protect the rights and freedoms of data subjects even when derogations apply. Moreover, use of the rights from which derogations are given must be 'likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes'.⁹³ Member States should tailor the scope of the derogations narrowly so that they will apply only when exercise of the rights in question would make the relevant data processing impossible or seriously impair it. Finally, the derogations only apply to the purposes mentioned in the respective paragraphs.⁹⁴ This means, for example, that when a company conducts scientific research then such data processing may fall under a derogation, but its subsequent use of the research results for commercial purposes would not. In practice, it may not always be easy to differentiate between the original research purposes of data processing and any subsequent purposes. It should be noted that the phrase 'in the public interest' in Article 89 modifies only 'processing for archiving purposes'; thus, data processing for scientific or historical research purposes or statistical purposes is covered by the Article even if they are not 'in the public interest'.

The derogations differ between processing for research and statistical purposes and for archiving in the public interest. For the former, Article 89(2) provides the possibility to introduce via Union or Member State derogations from the rights referred to in Articles 15 (right of access), 16 (right to rectification), 18 (right to restriction of processing) and 21 (right to object) GDPR. As noted, such derogations are still subject to the conditions and safeguards referred to in Article 89(1).

For archiving in the public interest, more derogations are possible. Article 89(3) allows for derogations via Union or Member State law from the rights referred to in Articles 15 (right of access), 16 (right to rectification), 18 (right to restriction of processing), 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing), 20 (right to data portability) and 21 (right to object) GDPR, conditioned on the existence of appropriate safeguards in accordance with Article 89(1). Thus, for archiving in the public interest specific derogations for the notification obligations of Article 19 and the right to data portability are possible that would not be permitted for processing for research or statistical purposes.

⁹² Rec. 156 GDPR.

⁹³ This formulation is used in both Art. 89(2) and (3) GDPR. Like for appropriate safeguards, it is not clear whether this has to be shown in a specific case or can be introduced in the abstract via Member State or Union law. Both options can be found in the national case law. See FN 88 above.

⁹⁴ See *ibid.*; Art. 89(4) GDPR.

For some data subject rights, no derogations are foreseen for either privileged purpose. This concerns the right to erasure (Article 17) and the right not to be subject to automated decision-making (Article 22). For erasure, a harmonised exception is provided in the text of Article 17 itself.⁹⁵ A similar provision was not made for the protections afforded in Article 22, which suggests they fully apply if the processing is based on one of the legal bases covered in the provision.⁹⁶

It is not clear how the derogations under Article 89(2) or (3) relate to the derogations to data subject rights possible under Article 23 GDPR. Under Article 23, all data subject rights can be restricted via Member State and Union law provided the conditions for such restrictions are followed. Importantly, the restriction has to serve one of the legitimate aims of Article 23(1), which are understood as an exhaustive list.⁹⁷ While there is no specific aim for archiving in the public interest, research or statistical purposes, it does not seem excluded that these purposes could be understood as ‘other important objectives of general interest’.⁹⁸ It seems therefore possible to introduce restrictions via Article 23 GDPR to rights not included for the respective privileged purposes in Articles 89(2) or (3), unless one argues that this contravenes the will of the legislator which might have wanted to introduce a specific regime superseding the one of Article 23 with Articles 89(2) or (3). Yet, in the absence of clear case law, this is far from the only defensible interpretation. Recital 156 actually suggests that for all privileged purposes Member States should be able to introduce ‘under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object’.⁹⁹ Thus, it does not introduce a distinction between processing for research and statistical purposes and archiving in the public interest, and suggests the derogations for archiving also apply to the other two purposes. This conflict between the recital and the text of Article 89 must be resolved in favour of the actual legal text, considering that the CJEU has already multiple times underlined the non-binding nature of recitals. Nevertheless, it adds to the confusion surrounding permissible derogations to data subject rights for the privileged purposes.

Finally, Article 89(4) makes clear that the derogations provided for in paragraphs (2) and (3) only apply to the purposes described in those paragraphs and not to any other purpose. In other words, in cases where a processing operation has multiple purposes, only the processing part corresponding to the privileged purpose will be able to benefit from any derogations for data subject rights.

5. Specific rules for archiving in the public interest, research, and statistics in other EU data laws

The GDPR is not the only law in the EU recognising that the use of data, including personal data, might be required for archiving purposes, research or statistical processing.¹⁰⁰ The EU’s open data framework, consisting of the Open Data Directive and the DGA, encourages the

⁹⁵ See Art. 17(3)(d) GDPR. See further the commentary on Art. 17 in this edition.

⁹⁶ Art. 22(2). See further the commentary on Art. 22 in this edition.

⁹⁷ See further the commentary on Art. 23 in this edition.

⁹⁸ Art. 23(1)(e) GDPR.

⁹⁹ Rec. 156 GDPR.

¹⁰⁰ EC Communication 2020, p. 6.

openness of research data,¹⁰¹ and archival data,¹⁰² while allowing for exceptions to its regime for statistical processing.¹⁰³ On the other hand, certain statistical data are earmarked for the designation as high-value datasets, meaning that Member States are required to collect certain statistical data and make them available.¹⁰⁴ The DGA supplements the approach of the Open Data Directive by introducing an optional system for sharing otherwise protected data and the idea of donating data for the public good, including for research, via data altruism.¹⁰⁵ It foresees exceptions for archives but explicitly encourages the making available of previously protected statistical data.¹⁰⁶ The framework for sharing more sensitive data includes a number of measures that could also be considered as appropriate safeguards for the purposes of Article 89(1), for example the idea of allowing for remote access to data only by using a ‘secure processing environment controlled by the public sector body’.¹⁰⁷

The DA provides a framework where data can be accessed, used and shared in full respect of European rules. Article 21 DA provides the possibility for public sector bodies to share data that was obtained in the context of an exceptional need with individuals or organisations carrying out scientific research or analytics, or with national statistical institutes and Eurostat for the compilation of official statistics. Such research activities should be compatible with the purpose for which the data was requested and the data holder should be informed about the further sharing of the data it has provided. The recitals (63, 64, 65, 76, and 115) further elucidate these exemptions, *inter alia* by explaining what can be understood under ‘exceptional need’, namely circumstances that are unforeseeable and limited in time.

Moreover, the DA introduces the concept of ‘data spaces’, a data governance framework to encourage data sharing, in particular for research purposes.¹⁰⁸ The European Commission is therefore currently supporting the establishment of a European Open Science Cloud, which should encourage the sharing of research data.¹⁰⁹ Similarly, the European Health Data Space Regulation, sets up a legal framework for the sharing of health data, *inter alia* for the purposes of research.¹¹⁰ The AIA contains an exemption from its provisions for AI research before the resulting AI system is put on the market or into service.¹¹¹

Article 40 DSA addresses the conditions under which data can be used for academic and research purposes, particularly when such data are derived from VLOPs (very large online platforms) and VLOSEs (very large online search engines). It supports the use of data to enhance public understanding of the impact of digital services on society. It also facilitates the access to data from VLOPs and VLOSEs for ‘vetted researchers’, enabling them to conduct studies on the societal impact of digital services, *inter alia* for the detection, identification and understanding of systemic risks and to assess the adequacy, efficiency and impacts of the risk

¹⁰¹ See rec. 27, 28 and Art. 9(2) Open Data Directive.

¹⁰² Art. 1(2)(d) Open Data Directive explicitly does not exclude archives from its scope. The Directive does foresee possibilities to facilitate the task of archives; e.g., they are allowed to charge higher fees for the access to documents. See rec. 38.

¹⁰³ Documents falling under statistical confidentiality are excluded, see Art. 1(2)(d) Open Data Directive.

¹⁰⁴ See further Commission Implementing Regulation High Value Data Sets, Annex, Area 4.

¹⁰⁵ See rec. 6, 16, 45, 50, and Arts. 2(16), 3, 5 and 16 to 25 Data Governance Act.

¹⁰⁶ See rec. 6, 7, 10 and 12 and Art. 3(1)(b) Data Governance Act.

¹⁰⁷ Rec. 7 and Art. 5(3)(b) Data Governance Act.

¹⁰⁸ Art. 33 Data Act.

¹⁰⁹ Data Strategy, pp. 15 and 33.

¹¹⁰ See rec. 1, 37, 38, 41, 67 and Art. 1 European Health Data Space Regulation.

¹¹¹ See rec. 25 and Arts. 2(6) and (8) AIA.

mitigation measures. The associated recitals (37, 96, 97, and 98) offer further guidance on these provisions.

Select Bibliography

International instruments

AI Framework Convention: Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, No. 225.

Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS No. 108.

Convention 108+: Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data 2018, CM/Inf(2018)15-final.

EU legislation

AIA: Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L 2024/1689, 12.7.2024.

Commission Implementing Regulation High Value Data Sets: Commission Implementing Regulation of 21 December 2022 laying down a list of specific high-value datasets and the arrangements for their publication and re-use, C/2022/9562 final.

DA: Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ 2023 L 2854.

DGA: Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ 2022 L 152/1.

DSA: Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ 2022 L 277/1.

European Health Data Space Regulation: Regulation of the European Parliament and of the Council on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847, PE-CONS 76/24, 8 January 2025.

GDPR: 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) (Text with EEA relevance), OJ 2016 L 119/1.

Horizon Europe Regulation: Regulation (EU) No. 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013, OJ L 170.

Open Data Directive: Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172.

Regulation 223/2009: Regulation (EC) No. 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No. 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No. 322/97 on Community Statistics, and Council Decision

89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities, OJ 2009 L 87/164.

Regulation (EU) No. 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC, OJ 2014 L 158/1.

National legislation

Austrian Federal Data Protection Act: Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl. I Nr. 165/1999 zuletzt geändert durch BGBl. I Nr. 24/2018.

Austrian Research Organisation Act: Bundesgesetz über allgemeine Angelegenheiten gemäß Art. 89 DSGVO und die Forschungsorganisation (Forschungsorganisationsgesetz – FOG) StF: BGBl. Nr. 341/1981 idF BGBl. Nr. 448/1981.

Belgian GDPR Implementation Law: Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, van 30 juli 2018; Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, du 30 juillet 2018.

Bulgarian Data Protection Act: Закон за защита на личните данни.

French Data Protection Act 1978: Act No. 78-17 of 6 January 1978 on Data Processing, Files and Individual Liberties (Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés), as last amended by Law No. 2014-334 of 17 March 2014.

French GDPR Implementation Law: Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.

French implementing decree: Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

German Federal Data Protection Act 2017: Bundesdatenschutzgesetz vom 30. Juni 2017, BGBl. 2017 Teil I Nr. 2097.

German Federal Cancer Registry Data Act: Bundeskrebsregisterdatengesetz.

Polish Personal Data Protection Act: Ustawa o ochronie danych osobowych.

Spanish Data Protection Act 2018: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y de Garantía de los Derechos Digitales.

Academic writings

Bentzen 2020: Bentzen, 'How to Assess What Constitutes 'Scientific Research' in the GDPR to Protect Data Subjects and Democracy' in Georgios Terzis, Dariusz Kloza, Elsbietta Kuzelewska and Daniel Trottier (eds.), *Disinformation and Digital Media as a Challenge for Democracy* (Intersentia 2020), 341.

Carmichael, Craddock and Stalla-Bourdillon 2023: Carmichael, Craddock and Stalla-Bourdillon, 'Art. 89 – Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes', in Spieker gen. Döhmman, Papakonstantinou, Hornung and De Hert, *General Data Protection Regulation: Article-by-Article Commentary* (Nomos 2023), 1113.

Comandé and Schneider 2022: Comandé and Schneider, 'It's time. Leveraging the GDPR to shift balance towards research-friendly EU data spaces', 59 *Common Market Law Review* (2022), 739.

Ctvrtník 2023: Ctvrtník, *Archives and Records: Privacy, Personality Rights, and Access* (Palgrave Maximillian, e-book 2023).

Edwards and Harbinja 2013: Edwards and Harbinja, 'Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World', 32(1) *Cardozo Arts & Entertainment law Journal* (2013), 101.

Erdos 2021: Erdos, 'Dead ringers? Legal persons and the deceased in European data protection law', 40 *Computer Law & Security Review* (2021), 1.

Forgó 2015: Forgó, 'My Health Data—Your Research: Some Preliminary Thoughts on Different Values in the General Data Protection Regulation', 5(1) *International Data Privacy Law 'IDPL'* (2015), 54.

Hallinan et al. 2020: Hallinan, Bernier, Cambon-Thomsen, Crawley, Dimitrova, Bauzer Medeiros, Nilsonne, Parker, Pickering, and Rennes, 'International transfers of health research data following Schrems II: A problem in need of a solution', SSRN (2020).

Harbinja 2023: Harbinja, *Digital Death, digital assets and post-mortem privacy* (Edinburgh University Press, e-book 2023).

Kotschy 2020: Kotschy, 'Article 6 Lawfulness of Processing', in Bygrave, Docksey and Kuner (eds.), *The EU General Data Protection Regulation (GDPR): a commentary* (Oxford University Press 2020), 321.

Pollicino 2021: Pollicino, 'Data Protection and Freedom of Expression Beyond EU Borders: EU Judicial Perspectives', in Fabbrini, Celeste and Quinn (eds.), *Data Protection beyond borders – Transatlantic perspectives on extraterritoriality and sovereignty* (Hart Publishing 2021), 81.

Pormeister 2017: Pormeister, 'Genetic Data and the Research Exemption: Is the GDPR Going too Far?', 7(2) *IDPL* (2017), 137.

Rouvroy and Pouillet 2009: Rouvroy and Pouillet, 'The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy', in Gutwirth et al (eds), *Reinventing data protection?* (Springer, e-book 2009), 45.

Rumbold and Pierscionek 2017: Rumbold and Pierscionek, 'The Effect of the General Data Protection Regulation on Medical Research', 19(2) *Journal of Medical Internet Research* (2017), 1.

Simitis 1981: Simitis, 'Data Protection and Research: A Case Study of Control', 29(4) *American Journal of Comparative Law* (1981), 583.

Staunton et al. 2022: Staunton, Slokenberga, Parziale and Mascalzoni, 'Appropriate Safeguards and Article 89 of the GDPR: Considerations for Biobank, Databank and Genetic research', (13) *Frontiers in Genetics* (2022), 719317.

Timmers et al. 2018: Timmers, van Veen, Maas and Kompanje, 'Will the EU Data Protection Regulation 2016/679 Inhibit Critical Care Research?', 27(1) *Medical Law Review* (2018), 59.

Woods 2021: Woods, 'Article 11 – Freedom of Expression and Information', in Peers, Hervey, Kenner, and Ward, *The EU Charter of Fundamental Rights* (Hart Publishing 2021), 333.

Papers of data protection authorities

AEPD and EDPS 2021: Agencia Española de Protección de Datos and European Data Protection Supervisor, '10 misunderstandings related to anonymisation' (27 April 2021).

EDPB 2019: European Data Protection Board, 'Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b))' (23 January 2019).

EDPB 2020A: European Data Protection Board, 'Guidelines 03/2020 on the processing of data concerning health for the purposes of scientific research in the context of the Covid-19 outbreak' (21 April 2020).

EDPB 2020B: European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' (4 May 2020).

EDPB 2021: European Data Protection Board, 'Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research' (2 February 2021).

EDPS 2020: European Data Protection Supervisor, 'A Preliminary Opinion on data protection and scientific research' (6 January 2020).

WP29 2014: Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (WP 216, 10 April 2014).

Austrian DPA 2021: Datenschutzbehörde, 'Order of 22 January 2021' (DSB-D124.1177/0006-DSB/2019).

Austrian DPA 2023: Datenschutzbehörde, 'Order of 21 June 2023' (2022-0.930.971).

Belgian DPA 2023: Autorité de protection des données/Gegevensbeschermingsautoriteit, 'Order of 19 December 2023' (DOS-2021-01986).

French DPA 2023: Commission Nationale de l'informatique et des Libertés, 'Order of 14 September 2023' (n° 2023-089).

Italian DPA 2023: Garante per la protezione dei dati personali, 'Order of 8 June 2023' (9921184).

Italian DPA 2024: Garante per la protezione dei dati personali, 'Order of 11 January 2024' (9977020).

Norwegian Privacy Appeals Board 2023: Personvernemnda, 'Appeal of 28 February 2023' (22/03062-5; PVN-2022-19).

Norwegian DPA 2023: Datatilsynet, 'Order of 26 April 2023' (22/03622-15).

Portuguese DPA 2022: Comissão Nacional de Proteção de Dados, 'Order of 12 December 2022' (2022/1072).

Spanish DPA 2021: Agencia Española de Protección de Datos, 'Order of 20 April 2021' (Nº: E/03690/2020).

Reports and recommendations

ALLEA et al. 2021: All European Academies, European Academies Science Advisory Council and Federation of European Academies of Medicine, 'International Sharing of Personal Health Data for Research' (April 2021).

Committee of Ministers of the Council of Europe 2000: Committee of Ministers of the Council of Europe, 'Recommendation No. R(2000) 13 of the Committee of Ministers to member states on a European policy on access to archives' (13 July 2000).

Consortium Oorlog voor de Rechter 2024: Consortium Oorlog voor de Rechter, 'De Oorlog Online: Handreiking voor het online beschikbaarstellen van archieven uit en over de Tweede Wereldoorlog' (March 2024).

Council of Europe 2016: Council of Europe, 'Recommendation CM/Rec(2016)6' (11 May 2016).

Data Strategy: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. A European strategy for data., COM(2020) 66 final, 19 February 2020.

EAG Guidelines 2018: European Archives Group, 'Guidance on data protection for archive services. EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector' (October 2018).

EC Study 2021: European Commission, 'Assessment of the EU Member States' rules on health data in the light of GDPR – Specific Contract No SC 2019 70 02 in the context of the Single Framework Contract Chafea/2018/Health/03' (February 2021).

European Commission 2021: European Commission, 'Ethics and Data Protection' (5 July 2021).

Friedewald, Székely and Karaboga 2024: Friedewald, Székely, and Karaboga, 'Access to archives in the digital age: Implementation of the Committee of Ministers of the Council of Europe Recommendation No. R (2000) 13 on a European policy on access to archives' (study commissioned by the Council of Europe, February 2024).

Hafner 2024: Hafner, 'Das Erinnern nicht vergessen: Der Datenschutz als Herausforderung für Archive der Schweiz. Eine Bestandsaufnahme' (Switzerland, March 2024).

Kindt et al. 2021: Kindt, Fontanilla López, Czarnocki, Kanevskaia, Herveg, and Benmayor, 'Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research' (Study for the EDPB, August 2021).

National Archives 2018: National Archives, 'Guide to archiving personal data' (United Kingdom, 2018).

Others

EDPB News 2021: European Data Protection Board, 'Slovenian Administrative Court upholds the decision of the Slovenian SA: the right of erasure does not enable an individual to have his data erased from Baptismal Register' (18 October 2021), available at https://www.edpb.europa.eu/news/national-news/2021/slovenian-administrative-court-upholds-decision-slovenian-sa-right-erasure_en.

FWO 2024: Research Foundation Flanders, 'Data Management Plan (DMP)' (accessed on 24 February 2025), available at <https://www.fwo.be/en/about-fwo/research-policy/data-management-plan-dmp/>.