2018 Draft commentaries on 10 GDPR articles
(from Commentary on the EU General Data Protection Regulation, OUP 2019)

Prof. Christopher Kuner, Vrije Universiteit Brussel
Prof. Lee Bygrave, University of Oslo
Christopher Docksey, Maastricht University
Prof. Dan Svantesson, Bond University
Prof. Cecile de Terwagne, University of Namur, et al.
Compilation from

Lee Bygrave/Christopher Docksey/Christopher Kuner,

*Commentary on the EU General Data Protection Regulation (GDPR)*

Forthcoming in 2019 from Oxford University Press

The following compilation includes a selection of non-final draft commentaries on ten 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 Please do not cite these working drafts.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

<table>
<thead>
<tr>
<th>Article</th>
<th>Topic</th>
<th>Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Territorial scope</td>
<td>Prof. Dan Jerker Svantesson, Bond University, Australia</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>Principles relating to processing of personal data</td>
<td>Prof. Cecile de Terwangne, University of Namur</td>
<td>19</td>
</tr>
<tr>
<td>6</td>
<td>Lawfulness of processing</td>
<td>Dr. Waltraut Kotschy, Data Protection Compliance Consulting, Vienna</td>
<td>32</td>
</tr>
<tr>
<td>17</td>
<td>Right to erasure ('right to be forgotten')</td>
<td>Dr. Herke Kranenburg,* Legal Service of the European Commission</td>
<td>57</td>
</tr>
<tr>
<td>20</td>
<td>Right to data portability</td>
<td>Dr. Orla Lynskey, London School of Economics and Political Science</td>
<td>68</td>
</tr>
<tr>
<td>24</td>
<td>Responsibility of the controller</td>
<td>Christopher Docksey, Maastricht University</td>
<td>82</td>
</tr>
<tr>
<td>25</td>
<td>Data protection by design and by default</td>
<td>Prof. Lee Bygrave, University of Oslo</td>
<td>99</td>
</tr>
<tr>
<td>46</td>
<td>Transfers subject to appropriate safeguards</td>
<td>Prof. Christopher Kuner, Vrije Universiteit Brussel (VUB), Brussels</td>
<td>108</td>
</tr>
<tr>
<td>56</td>
<td>Competence of the lead supervisory authority</td>
<td>Dr. Hielke Hijmans, Centre for Information Policy Leadership (CIPL), Considerati Amsterdam, Vrije Universiteit Brussel (VUB), Brussels</td>
<td>123</td>
</tr>
</tbody>
</table>

*The views expressed are solely those of the authors and do not necessarily reflect those of the European Commission.
**Article 3**

**Territorial scope**

*Prof. Dan Jerker Svantesson*

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
   (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

**Relevant recital**

(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.

(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

*Svantesson*
(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

(25) Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

CLOSELY RELATED PROVISIONS

Article 2 (Material scope) (see too recitals 13-21 & 27); Articles 44-50 (Transfer of personal data to third countries or international organisations) (see too recitals 101-116); Articles 55-58 (Competence, tasks and powers) (see too recitals 122-124, 127-129, 131-133 & 137); Article 79 (Right to an effective judicial remedy against a controller or processor) (see too recitals 141, 145 & 147)

RELATED ARTICLES IN EPD [Directive 2002/58/EC]

Articles 1 (scope and aim) and 3 (services concerned) partially have a somewhat similar effect in referring to ‘data and of electronic communication equipment and services in the Community’ respectively ‘the provision of publicly available electronic communications services in public communications networks in the Community’ (emphasis added in both quotes)

RELEVANT CASE LAW

CJEU

Case C-131/12, Google Spain v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014 (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).
A. Rationale and Policy Underpinnings

Article 3 delineates the Regulation’s scope of application, purportedly in a spatial sense. Yet, to understand the rationale underpinning Article 3, we must start by recognising that the Article’s rubric ‘Territorial scope’ should not be taken literally. Disregarding occasional expansions, and events such as ‘Brexit’, the EU’s territory is stable, (largely) undisputed and measurable in square meters. However, it is not that territorial scope to which the Article relates. Rather, Article 3 outlines what types of contact with the EU’s territory will activate the application of the GDPR, and it does so in a manner that is partly territoriality-dependent and partly territoriality-independent.

Already from the outset, it was clear that a key policy driving, as well as justifying, the data protection reform that resulted in the GDPR was a perceived need to expand the scope of application of the EU’s data protection law. Such an expansion was argued to ensure a ‘level playing-field’ as to between businesses based in the EU and businesses based outside the EU, but doing business on the European market. This, it was suggested, would lead to fair competition in a globalised world. While this thinking may be criticised as unnuanced and unrealistic in that compliance with the GDPR as a whole is likely to be prohibitively expensive for many controllers and processors not established in the Union, and while some may thus see the GDPR’s broad scope of application rather as anti-competitive in a globalised world, the policy expressed in this thinking must be noted as it potentially will impact the practical application of Article 3. Put somewhat simplistically, this policy aim points to a likelihood of the article being given a broad reach.

However, it must be recalled that a key purpose of Article 3 is to position the GDPR within the international system. And in this context, clear guidance is provided by the Commission, in the form of its amicus brief filed in relation to the matter between the United States of America and Microsoft Corporation (the Microsoft Warrant case) heard in the Supreme Court of the United States on 27 February 2018. There, the Commission refers to Arts. 3(5) and 21(1) TEU, Case C-52/69, Geigy v. Commission, and Case C-366/10, Air Transport Ass’n of America v. Sec’y of State for Energy and Climate Change, and notes:

> Any domestic law that creates cross-border obligations—whether enacted by the United States, the European Union, or another state—should be applied and interpreted in a manner that is mindful of the restrictions of international law and considerations of international comity. The European Union’s foundational treaties and case law enshrine the principles of “mutual regard to the spheres of jurisdiction” of sovereign states and of the need to interpret and apply EU legislation in a manner that is consistent with international law.

This proclamation may no doubt be seen as the key to understanding the proper application of Article 3, and clearly calls for a degree of restraint in recognition of the interests of foreign states and the international order. Indeed, this proclamation draws

---

1 See Reding 2014; a similar sentiment is expressed by Albrecht 2016, p. 476.
2 Case C-52/69, Geigy, at para 11.
3 Case C-366/10, Air Transport, at para 123.
4 EC Microsoft brief, p. 7.
attention to the fact that a provision such as Article 3 is designed, not only to maximise the implementation of the policy goals pursued in the GDPR, but also to ensure that the harmonious co-existence between different legal systems.

Finally, it is worth emphasising the importance of the very fact that a provision like Article 3 is included in the GDPR. While quite common, not all data protection schemes include a provision aimed at clarifying the scope of application. Further, not all EU instruments include a provision aimed at clarifying the scope of application. The inclusion of an Article like Article 3 is useful and as noted by Jääskinen and Ward it is good practice for the ‘EU legislature to address the external reach of measures of EU private law in the individual measures themselves, whether that be a regulation or a directive’5.

B. Legal Antecedents

1. EU legislation

Article 3’s predecessor in the DPD is Article 4. It reads as follows:

Article 4 - National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
   (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
   (b) the controller is not established on the Member State’s territory, but in a place where its national law applies by virtue of international public law;
   (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

2. International treaties

There are no international treaties that specifically and expressly regulate the scope of application of data protection laws. However, it should be noted that: ‘EU data protection law is based largely on fundamental rights law so that the permissibility of

extraterritoriality in data protection depends largely on the extraterritorial scope of EU fundamental rights instruments. As a consequence, several international treaties impact Article 3 indirectly. For example, according to Article 13 ECHR: ‘Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.’

Furthermore, Article 1 of the current version of the Council of Europe’s Convention 108 is relevant: ‘The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him (‘data protection’).’

Finally, the fact that the application of the GDPR will impact the human rights of non-EU individuals is of great significance; it means that in assessing the human rights implications of the GDPR account must be taken of human rights law beyond Europe’s human rights law.

Article 2(1) of the International Covenant on Civil and Political Rights (ICCPR) states:

Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Arguably, the phrase ‘to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant’ expresses two separate requirements rather than a double requirement. From that vantage point, each signatory state has an obligation to provide legal protection against unlawful attacks on the rights of people subject to its jurisdiction and those present within its territory, regardless of the origins of the attacks.

3. National legislation

Being of central importance in any data protection legislation, provisions delineating the territorial scope of application are commonly found in national legislations. An example of the national implementation of Article 3’s predecessor in the DPD (Article 4) can be found in Section 4 of the Swedish Personal Data Act:

This Act applies to those controllers of personal data who are established in Sweden. The Act is also applicable when the controller of personal data is established in a third country but for the processing of the personal data uses equipment that is situated in Sweden.

---

6 Kuner 2015, p. 243.
7 Svantesson 2014, p. 78.
However, this does not apply if the equipment is only used to transfer information between a third country and another such country.

In the case referred to in the second paragraph, first sentence, the controller of personal data shall appoint a representative for himself who is established in Sweden. The provisions of this Act concerning the controller of personal data shall also apply to the representative.8

4. Case law

On a few occasions, the CJEU has had reason to rule directly on the subject matter of Article 3 (but of course in the context of Article 4 DPD). One example is its judgment in the Google Spain case. The reason the Google Spain case gave rise to Article 4 considerations is found in the fact that Google argued that the local branch of Google (in this case, Google Spain) being within the reach of the local law did not automatically mean that the US-based Google Inc, that operates the company’s well-known search engine, would be. The CJEU concluded that “the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked”9 meaning that also Google Inc falls within the ambit of Article 4(1)(a) DPD (and presumably Article 3(1) of the Regulation). This conclusion was justified by reference to the objective of Directive 95/46 and of the wording of Article 4(1)(a), as well as the fact that Google Spain is intended to promote and sell, in Spain, advertising space to make the service offered by Google Inc profitable — thus, meeting the test of the the processing being carried out in the context of the activities of an establishment of the controller on the territory of the Member State (in this case, Spain), articulated in Article 4(1)(a) DPD.

The wider impact of the Google Spain case – as far as the territorial scope is concerned – must be read in conjunction with the CJEU’s decision (and Advocate General Saugmandsgaard Øe’s Opinion) in Verein für Konsumenteninformation. In that matter, the CJEU concluded that Article 4(1)(a) DPD must be interpreted as meaning that the processing of personal data carried out by an undertaking engaged in electronic commerce is governed by the law of the Member State to which that undertaking directs its activities, if it is shown that the undertaking carries out the data processing in question in the context of the activities of an establishment situated in that Member State. The CJEU also emphasised that it is for the national court to ascertain whether that is so.10 Importantly, Advocate General Saugmandsgaard Øe emphasised that, the reason the CJEU in Google Spain gave such a broad interpretation to Article 4(1)(a) DPD was to avoid that the processing in question would escape the obligations laid down in the DPD.11 Thus, such a broad interpretation might not be legitimate where such a risk is not present. On the other hand, in Case C 210/16, Advocate General Bot expressed the view that: ‘The fact that, by contrast with the situation in the case which gave rise to the judgment of 13 May 2014, Google Spain and Google, […] the Facebook group has a European head office, in Ireland, does not mean that the interpretation of Article 4(1)(a) of Directive 95/46

---

8 Swedish Personal Data Act, section 4.
9 Case C-131/12, Google Spain, at paras 55-56.
10 Case C-191/15, Verein für Konsumenteninformation, at para. 82.
11 Case C-191/15, Verein für Konsumenteninformation (AG Opinion), at paras 124-125.
which the Court adopted in that judgment cannot be applied in the present case. Consequently, this matter remains to be adequately clarified.

_Weltimmo_ involved a blatant instance of a business in one Member State (Slovakia) being set up to engage only in business in another Member State (Hungary). In discussing the meaning of the term ‘establishment’, the CJEU noted that, while the owner resided in Hungary, _Weltimmo_ was registered in Slovakia and was, therefore, established there within the meaning of company law. However, _Weltimmo_ carried out no activity in Slovakia but had representatives in Hungary. _Weltimmo_ had opened a bank account in Hungary and had a letter box there for its everyday business affairs. The property website which constituted its main business was written exclusively in Hungarian and dealt only with properties in Hungary. All this suggests that _Weltimmo_ had a substantial connection to Hungary and that Hungary had a legitimate interest in the matter. It also suggests that the actual link to Slovakia — the place of registration — was comparatively weak.

In the light of this, the CJEU held that _Weltimmo_ pursued a real and effective activity in Hungary, and the Court stressed the need for a flexible definition of the concept of ‘establishment’, rather than a formalistic approach whereby undertakings are established solely in the place where they are registered:

> Article 4(1)(a) . . . must be interpreted as permitting the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity — even a minimal one — in the context of which that processing is carried out... 

Expanding upon this point, the CJEU also noted:

> [I]n order to ascertain, in circumstances such as those at issue in the main proceedings, whether that is the case, the referring court may, in particular, take account of the fact (i) that the activity of the controller in respect of that processing, in the context of which that processing takes place, consists of the running of property dealing websites concerning properties situated in the territory of that Member State and written in that Member State’s language and that it is, as a consequence, mainly or entirely directed at that Member State, and (ii) that that controller has a representative in that Member State, who is responsible for recovering the debts resulting from that activity and for representing the controller in the administrative and judicial proceedings relating to the processing of the data concerned...

The Court added that, by contrast, the issue of the nationality of the persons concerned by such data processing is irrelevant.

---

12 C-210/16, _Unabhängiges Landeszentrum_ (AG Opinion), at para 95.
13 Case C-230/14, _Weltimmo_, at para. 41.
14 Ibid., at para. 41.
15 Ibid., at para. 41.
C. Analysis

Article 3 outlining the Regulation’s territorial scope is one of the most important parts of the Regulation; after all, unless the criteria set out in Article 3 are met, the Regulation simply does not apply and none of the other Articles are of relevance. Especially for data controllers, processors and subjects outside of the EU, Article 3 ought to be the first provision of the Regulation that they consult. To this may be added that delineating the territorial reach of an instrument such as the GDPR is a complex task, and while it seems clear that Article 3 represents an expansion of the reach of EU’s data protection law (compared to how Article 4 DPD was applied), the actual scope of application catered for under Article 3 is far from clear. In the light of this, it is highly unfortunate, and indeed surprising, that while the Article 29 Working Party has issued Guidelines on a range of other aspects of the GDPR, no Guidelines had been issued as of early May 2018. The closest we come is the following brief statement included in the Article 29 Working Party’s general factsheet aimed at helping Asia Pacific Privacy Authorities understand the basic requirements included in the GDPR:

The GDPR applies to data controllers and data processors with an establishment in the EU, or with an establishment outside the EU that target individuals in the EU by offering goods and services (irrespective of whether a payment is required) or that monitor the behavior of individuals in the EU (where that behavior takes place in the EU). Factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

Data controllers and/or data processors not established in the EU, but whose activities fall within the scope of the GDPR, will generally (some exceptions apply) have to appoint a representative established in an EU member state. The representative is the point of contact for all Data Protection Authorities (DPAs) and individuals in the EU on all issues related to data processing (Article 27).16

Perhaps the most significant aspect of this statement is its specific inclusion of the phrase ‘target individuals in the EU’. In the Article 29 Working Party’s general factsheet aimed at helping Asia Pacific Privacy Authorities we also find the following example illustrating the practical application of Article 3: ‘A Japanese web shop, offering products, available online in English with payments to be made in Euros, processing multiple orders a day from individuals within the EU and shipping these products to them, should be compliant with the GDPR’.17

Unfortunately, this example raises more questions than it answers. We may, for example, wonder whether the Japanese web shop in question would avoid the GDPR simply by only accepting payment in non-EU currencies? And what if the Japanese

17 Ibid.
web shop, rather than “processing multiple orders a day from individuals within the EU”, merely accept such orders occasionally, or once a day? What are the actual thresholds that will be applied?

At any rate, given the combination of Article 3’s complexity and resulting uncertainty on the one hand, and its central importance on the other hand, it is only natural if litigation arises in relation to Article 3 over the Regulation’s early years of operations.

From an analytical perspective, Article 3 may be broken down into three parts. The first (Article 3(1)), ensures that the Regulation applies to the processing of personal data by a controller or a processor with an establishment in the Union. The second (Article 3(2)), extends the Regulation’s application to a controller or a processor that lack an establishment in the Union, under certain defined circumstances. The third (Article 3(3)), addresses specific situations where Member State law applies by virtue of public international law.

While it is worth mentioning that Article 3 focuses on events and persons ‘in the Union’ in contrast to Article 4’s DPD focus on events and persons ‘on the territory of the Member State’, it may perhaps be presumed that this is not intended to change anything. In this context, it should be noted that the GDPR also applies e.g. in Guadeloupe, French Guiana, Martinique, Réunion, Saint-Barthélemy, Saint-Martin, the Azores, Madeira, and the Canary Islands, as well as in the Åland Islands. However, as noted by Jääskinen and Ward: ‘The special arrangement of association with the EU, as prescribed by Article 355(2) TFEU, has spawned a complex body of case law on the circumstances in which EU law extends to the associated countries, given that they inevitably entail assessment of conduct and legal relations that have occurred outside of EU territory.’ In addition, it should be observed that the GDPR will be implemented in the three states – Norway, Iceland, and Liechtenstein – that are part of the European Economic Area (EEA) Agreement, but not Member States of the EU.

Article 3(1) adopts largely the same focus on processing of personal data in the context of the activities of an establishment of a controller in the Union, as did Article 4(1)(a) DPD. Consequently, the CJEU’s decisions in Weltimmo, Google Spain and Verein für Konsumenteninformation (discussed above) likely set important precedents for the operation of the Regulation. Yet, while the similarity between Article 4(1)(a) of the DPD and Article 3(1) of the Regulation are obvious, so too are the differences. For example, while Article 4(1)(a) of the Directive specifically addresses situations where the same controller is established on the territory of several Member States, Article 3(1) of the Regulation does not do so. Under the Regulation, such situations are instead addressed in other provisions (see in particular Article 56). Furthermore, while Article 4(1)(a) DPD only referred to the activities of an establishment of the controller, GDPR Article 3(1) the processing of personal data in the context of the activities of an establishment of a controller or a processor.

---

18 Art. 355(1) TFEU.
19 Art. 355(4) TFEU.
20 Jääskinen and Ward 2016, p. 129. For all different territories see Annex II TFEU.
Another difference can be deduced from Advocate General Cruz Villalón’s discussion in *Weltimmo*, clarifying the complex operation of Article 4(1) DPD. He points to that Article’s dual function:

On the one hand, it [Article 4(1)(a)] enables the application of EU law through the law of one of the Member States where data processing is carried out solely ‘in the context’ of the activities of an establishment situated in that Member State, even though, strictly speaking, the processing is carried out in a non-member country (as was the case in *Google Spain and Google*). On the other hand, that provision operates as a rule for determining the applicable law as between Member States (which is the question at issue in the present case). In the latter situation, Article 4(1)(a) of the directive is the provision which determines the applicable law in so far as it is a rule governing conflict between the laws of the different Member States.\(^{21}\) (internal footnote omitted)

The second of these functions – that of operating as a rule for determining the applicable law as between Member States – may be called into question as far as Article 3(1) is concerned. After all, with a Regulation, as opposed to a Directive, the question of applicable law should, generally, not matter.

Finally, Article 3(1), unlike Article 4(1)(a) DPD, expressly states that the Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, *regardless of whether the processing takes place in the Union or not*. And in this context, it is prudent to recall that, it is not the location of the data that is the criterion used under EU data privacy law to define its territorial scope: ‘The WP29 stresses that the location of the data is not the criterion used under the GDPR to define its territorial scope.’\(^{22}\)

Article 3(2) is fundamentally different from its predecessor in the DPD (Article 4(1)(c)). Instead of focusing on the use of equipment situated in the EU (as did Article 4(1)(c) DPD), Article 3(2) describes two circumstances under which the Regulation applies to a controller or processor not established in the Union. A requirement shared by both those circumstances is that the processing must be of personal data of data subjects who are in the Union.

Article 3(2)(a) ensures that the Regulation applies to a controller or processor not established in the Union where it is offering goods or services to data subjects in the Union. Importantly, the application of the Regulation does not depend on whether a payment of the data subject is required. Thus, the Regulation extends to ‘free’ goods or services, which is a particularly important matter in the online context. Article 3(2)(b) ensures that the Regulation applies to a controller or processor not established in the Union where it is monitoring the behaviour of data subjects in the Union, as far

\(^{21}\) Case C-230/14, *Weltimmo* (AG Opinion), at para. 23.

\(^{22}\) WP29, Statement on electronic evidence, Brussels, p. 5. The Article 29 Working Party is clearly correct and it is unfortunate that several MEPs who have worked closely on the GDPR have sought to place focus on the location of data in their *amicus* brief filed in relation to the *Microsoft Warrant* case. See: Albrecht Microsoft brief, claiming that the EU data protection regime was ‘specifically intended and designed to cover data stored in an EU Member State.’ (at 14), and that ‘Personal data located in EU territory is subject to strict rules designed to maintain the autonomy of the affected individual (the “data subject”)’ (at 5).
as their behaviour takes place within the Union. Thus, Article 3(2)(b) is even broader in scope than is Article 3(2)(a) and is likely to capture a diverse range of both online and offline activities.

Some guidance as to the likely application of Article 3(2) can be discerned from recitals 23 and 24. The recitals make clear that the drafters of Article 3 are seeking to leverage the ‘targeting’ test that has started to play an increasing role in EU consumer protection law, predominantly via the joined CJEU decisions in Pammer.23 Drawing upon legal solutions from other fields is sensible, and consumer protection law shares several key features with data privacy law. In addition, the targeting test is frequently trumpeted as a solution to Internet jurisdiction issues. Yet, while targeting is attractive in theory, on a practical level, applying this test in the context of Article 3(2) will not be easy and will not necessarily cater for any high degree of predictability for data subjects, controllers, processors or, indeed, data protection authorities.

A key challenge here is the limited number of what we may call ‘indicators of targeting’. In Pammer, the CJEU discussed a non-exhaustive list of indicators such as the mention of telephone numbers with the international Code, the use of a certain language and/or currency and the use of a certain top-level domain name as potentially indicating that the party in question had targeted the relevant Member State. However, these indicators of targeting may be missing or be irrelevant, for example, in the context of assessing whether a controller or processor not established in the Union is offering free services to data subjects in the Union. Thus, there is a clear risk that, for a large number of controllers and processors, courts are going to have to conclude either that they ‘target’ just about every country in the world or no countries at all. Both of these options are serious impediments for the practical usefulness of the targeting approach adopted in Article 3. Another potential complication arises out of the focus on subjective targeting, as opposed to objective targeting. Recital 23 refers to it being ‘apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union’ (emphasis added). This suggests that it is what is in the mind of the controller or processor that matters, rather than whether targeting occurs from an objective perspective.

In this context, it is important to observe that, while the recitals clearly impose an expressed intention requirement in relation to Article 3(2)(a), it equally clearly does not include any expressed such requirement in relation to Article 3(2)(b). Based on this difference, it may be argued that also unintentional monitoring may be caught by Article 3(2)(b).

At the same time, recital 24 makes clear that, when seeking to ascertain whether certain conduct amounts to monitoring, we must take account of the potential subsequent use of personal data processing techniques which consist of profiling a natural person. Thus, it may, for example, be argued that, where the monitoring is unintentional and is carried by an entity that does not associate the collected data with any potential data processing techniques which consist of profiling a natural person, that entity is not caught by Article 3(2)(b).

23 Joined Cases C-585/08 and C-144/09, Pammer.
In the light of these different possible interpretations, it must be concluded that there is a pressing need for detailed guidance as to the proper application of Article 3(2)(b). Until such guidance is provided, uncertainty remains an obstacle for compliance.

Turning to Article 3(3), three observations can be made: first, it largely mirrors Article 4(1)(b) of the DPD, and second, recital 25 suggests that it is aimed at data processing e.g. in the context of a Member State's diplomatic mission or consular post. Third, while the text of the relevant recital (25) indicates that Article 3(3) will have a limited scope of application, the text itself gives it a tremendous potential for an expansive reach.

Given that Article 3(3) is nearly identical to Article 4(1)(b) of the DPD, it may perhaps be assumed that it was included without much thought or analysis. This is unfortunate since neither Article 3(3) GDPR, nor Article 4(1)(b) DPD, actually cater for the GDPR/DPD applying to a Member State's diplomatic mission or consular post as anticipated in the recital.

The DPD assumed, and the GDPR now assumes, that public international law results in Member State law applying to data processing in its diplomatic missions and consular posts. However, this is assumption is wrong.

It is true that diplomatic staff enjoy certain privileges and immunities. However, while Grotius and his contemporaries argued that ambassadors were deemed to be outside the territory of the host State, ‘it is now widely acknowledged that diplomatic premises are not part of foreign territory.’ To this may be added that, Article 41 of the Vienna Convention on Diplomatic Relations states: ‘Without prejudice to their privileges and immunities, it is the duty of all persons enjoying such privileges and immunities to respect the laws and regulations of the receiving State.’ Given the above, the majority view in contemporary public international law does not support the assumption that Member State law automatically applies to data processing in its diplomatic missions and consular posts.

Of course, diplomatic agents and diplomatic missions are inviolable, so the receiving State has little, or no, practical means to compel compliance with its local law. However, the local law still applies as such. Thus, the GDPR’s assumption that, for example, French data protection law automatically applies in the French embassy in Washington as a matter of public international law is incorrect.

The other side of this coin potentially has even greater implications. Foreign States may, based on recital 25, have believed that the GDPR would not extend to apply to their diplomatic missions and consular posts in the EU. However, in the light of the above, it would seem that such bodies are indeed caught by Article 3(1), and in that context, the assertion that the Regulation applies regardless of whether the processing takes place in the Union or not, may be a particularly controversial matter.

24 See: Art. 29 Vienna Convention on Diplomatic Relations.
25 Art. 22 Vienna Convention on Diplomatic Relations.
26 d’Aspremont 2009, para 3.
27 WP29 2010, p. 18.
It is no doubt desirable that the GDPR applies to Member States’ diplomatic missions or consular posts as is anticipated in recital 25. However, it seems that the only way in which we can reconcile the wording of Article 3(3) with this aim is to argue that, since public international law allows nationality-based prescriptive jurisdiction, the EU has the right to extend the application of the GDPR to the Member States’ diplomatic missions or consular posts, and that it does so via recital 25. The fact that the Member States’ diplomatic missions or consular posts also have to respect local law does not necessarily stand in the way of such an argument. This far-fetched approach would, however, require an extraordinarily broad reading of the phrase ‘where Member State law applies by virtue of public international law’ by assuming this to refer to any place where public international law allows Member State law to apply. In other words, the phrase ‘applies by virtue of public international law’ would have to be read to mean ‘is permitted to be applied under public international law’. I strongly caution against such an interpretation, and conclude that neither Article 3(3), nor the other subsections of Article 3, extends the GDPR to operate in a Member State’s diplomatic mission or consular post. In this respect, Article 3 is then too limited and fails to give the GDPR its intended reach of operation.

To understand the potential reach of Article 3(3)’s claim that the Regulation applies to controllers (but apparently not processors) not established in the Union but in ‘a place where Member State law applies by virtue of public international law’, we must understand the extent to which public international law places restrictions on the reach of so-called prescriptive (or legislative) jurisdiction. The wording of Article 3(3), and of the recital, seems to assume that public international law provides a clear delineation in this respect. However, such an assumption is erroneous. Public international law does not provide clear guidance as to the exact reach of prescriptive jurisdiction. This gives rise to a structural issue. Public international law provides for a wide discretion as to where states claim prescriptive jurisdiction, but through Article 3(3) the EU asserts that the scope of the Regulation is determined by public international law. This circularity means that the Regulation tells us to consult public international law, while public international law – due to the discretions it affords – tells us to primarily seek guidance in the Regulation.

Furthermore, even if we were to settle for a superficial assessment and accept the principles advanced through the influential 1935 ‘Harvard Draft’ (possibly accompanied by the so-called ‘effects doctrine’) as representing the view of public international law on the matter, we would have to conclude that Article 3(3) entitles the EU to apply the Regulation broadly indeed. And, as is well known, not all the ‘Harvard Draft’ principles are focused on territoriality, which adds to the sense that the heading of Article 3 – territorial scope – is somewhat misguided.

We can, however, get out of this quagmire and regain firm ground if it is accepted that, in referring to ‘a place where Member State law applies by virtue of public international law’, Article 3(3) includes only those places where public international law causes Member State law to apply, at that place, on a permanent basis, as opposed to Member State law being applicable merely as a result of the public international law principles commonly used specifically to allocate prescriptive jurisdiction. Where

---

28 Svantesson 2017, p. 43.
29 ‘Introductory Comment’ 1935.
this is accepted, we avoid the risk of Article 3(3) getting an overly expansive meaning so as to make the GDPR applicable based e.g. on nothing but the fact that some effect was felt in a Member State or based on the nationality of the controller.

Taken as a whole, Article 3 – and in particular Article 3(2), and potentially Article 3(3) – clearly casts a wide net indeed, and this has at least four important consequences. First of all, as already alluded to, the broad theoretical reach of Article 3 makes it difficult to predict its actual practical reach. Second, it is possible to argue that Article 3 – and again, in particular Article 3(2), and potentially Article 3(3) – goes too far, thereby giving the GDPR a scope of application that is difficult to justify on the international stage as the GDPR may end up applying in situations in relation to which the EU may be argued to lack a legitimate interest to apply its laws and to which the EU has only a very weak connection. Third, the fact that the GDPR – through Article 3 – purports to apply so broadly that it is not possible to ensure actual enforcement of the Regulation to all that it applies to, means that enforcement will necessarily be selective and thereby at the risk of being viewed as subjective and, indeed, discretionary. This raises rule of law concerns and arguably undermines the GDPR’s international legitimacy. Fourth, flowing from the first three observations, it is desirable (not to say necessary) to develop clear guidance as to when a controller or processor not established in the Union will actually be pursued under the GDPR. This may perhaps best be a task for the European Data Protection Board.

In the context of guidance as to when a controller or processor not established in the Union will actually be pursued under the Regulation, it would seem fruitful to embrace a proportionality approach that goes beyond mere attention given to the criteria set in Article 3. For example, it can perhaps be expected that attention will be given to the degree of harm caused (or potentially caused) as well as the type of provision of the Regulation that is alleged to have been violated. This may, for example, be achieved via what may be referred to as a ‘layered approach’; \(^{30}\) that is, when determining whether to actually pursue an alleged violation by a controller or processor not established in the Union, the degree of contact required should be proportionate to the degree of harm caused, as well as the type of provision of the Regulation that is alleged to have been violated. Under such a model for the application of Article 3, a violation of an Article belonging to the more administrative/bureaucratic layer of the Regulation (such as Article 37 requiring a Data Protection Officer) could require a stronger degree of contact with the EU than, for example, a violation of the lawfulness requirements in Article 6 causing significant damage. This would give Article 3 a nuanced application despite its, complex yet unsophisticated, ‘all-or-nothing’ literal meaning. And this nuanced application is clearly supported by the Commission’s call – discussed above – for domestic law that creates cross-border obligations to be applied and interpreted in a manner that is mindful of the restrictions of international law and considerations of international comity, in the light of how the European Union’s foundational treaties and case law enshrine the principles of ‘mutual regard to the spheres of jurisdiction’ of sovereign states and of the need to interpret and apply EU legislation in a manner that is consistent with international law.

\(^{30}\) Svantesson 2013.
Select Bibliography

Legislation


Case law


Academic writings


Czerniawski, ‘Do We Need the “Use of Equipment” as a factor for the territorial applicability of the EU Data Protection Regime?’ in D. Svantesson and D. Kloza (eds), *Trans-Atlantic Data Privacy as a Challenge for Democracy* (Intersentia 2017), 221.


Kindt, ‘Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation’, 32 *CLSR* (2016), 729.


*Papers of data protection authorities*


Others

Article 5

Principles relating to processing of personal data

Prof. Cécile de Terwangne

1. Personal data shall be:
   (a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
   (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
   (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
   (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
   (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; 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 organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);
   (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

Relevant recital

(39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation
to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

CLOSERLY RELATED PROVISIONS

Article 6(1) (Lawfulness of processing) (see too recitals 40 to 49); Article 6(4) (exceptions to the requirement of compatible purposes for further processing and criteria to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected) (see too recital 50); Article 12 (transparent information) (see too recitals 58, 60 and 61); Article 24 (responsibility of the controller) (see too recitals 74 to 77); Article 32 (security of processing) (see too recital 83); Article 89(1) (safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes) (see too recitals 158 to 163)

RELATED ARTICLES IN LED [Directive (EU) 2016/680]

Article 4 (Principles relating to processing of personal data) (see too recitals 26 to 28); Article 9(1-2) (Specific processing conditions) (see too recital 34); Article 13 (Information to be made available or given to the data subject) (see too recitals 39, 40 and 42); Article 19 (Obligations of the controller) (see too recitals 50-51); Article 29 (Security of processing) (see too recital 60)

RELEVANT CASE LAW

CJEU

Joined Cases C-92/09 and 93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, judgment of 9 November 2010 (ECLI:EU:C:2010:662).
Case C-342/12, Worten – Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT), judgment of 30 May 2013 (ECLI:EU:C:2013:355).
Case C-291/12, Michael Schwarz v. Stadt Bochum, judgment 17 October 2013 (ECLI:EU:C:2013:670).
Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Kärntner Landesregierung, Seitlinger and Others, judgment of 8 April 2014 (ECLI:EU:C:2014:238).
Case C-201/14, Smaranda Bara and Others v. Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF), judgment of 1 October 2015 (ECLI:EU:C:2015:638).
Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, judgment of 21 December 2016 (ECLI:EU:C:2016:970).

ECtHR

A. Rationale and Policy Underpinnings

Article 5 lays down all the key principles setting up the protection of personal data: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. Certain principles are further developed in other parts of the Regulation. That is the case for the transparency principle which takes the form of a duty to inform data subjects (Articles 12 and following) as well as for the security rules (Article 32) and for the accountability principle (Article 24).

Data protection fundamental principles have not been modified compared with the other rules governing this field for several decades. The principles laid down in the 1980 OECD Guidelines and in the 1981 Convention 108 of the Council of Europe have demonstrated their capacity to stand the test of time. ‘More than 30 years of practical application have proven these principles to be sound’. These principles could indeed be applied in different technical, economic and social contexts. ‘So far nobody has been able to claim convincingly that the substantial principles of data protection as contained in Article 6 of the Data Protection Directive—and in Article 5 of the Convention—must be amended.’ In consequence, the GDPR does not make fundamental changes to these basic data protection principles. However certain adjustments and additions have been made in the GDPR, as we will see in the following discussion.

B. Legal Antecedents

1. EU legislation

Article 6(1) DPD contains virtually the same principles as Article 5 GDPR. It is entitled ‘Principles relating to data quality’, although it deals with more than just data quality. It does indeed state principles relating to the lawfulness and fairness of processing; purpose limitation; data minimisation; the accuracy of data; and storage limitation. All these principles are stated in terms very similar to the GDPR. Contrary to Article 5 GDPR, Article 6 DPD does not mention the principle of integrity and confidentiality, which is logical since this provision is dedicated to data quality – even if certain principles contained therein go beyond the mere question of data quality. In contrast Article 5 is entitled ‘Principles relating to processing of personal data’ and has a wider scope. Provisions on the integrity and confidentiality of processing are to be found in DPD Articles 16 and 17. No accountability principle is stated as such but Article 6(2) DPD clarifies all the same that ‘It shall be for the controller to ensure that paragraph 1 is complied with’.

2. International treaties

The fundamental principles relating to data protection have been set forth from the very beginning in the international instruments protecting individuals with regard to processing of personal data. Article 5 of Convention 108 inspired Article 6 DPD,
which virtually replicates its provisions adding certain complements, and which in
turn has served as a basis for Article 5 GDPR. Article 5 of Convention 108 contains
the same principles relating to the lawfulness and fairness of processing; purpose
limitation; data minimisation; accuracy of data; and storage limitation. Article 7 enti-
tled ‘Data security’ requires appropriate security measures to be taken for the protec-
tion of personal data ‘against accidental or unauthorised destruction or accidental loss
as well as against unauthorised access, alteration or dissemination’. There is no trace
of the accountability principle in the Convention. The revised text of the Convention
brings certain new elements on these last two points. The security requirement is
slightly rewritten to state that: ‘Each Party shall provide that the controller, and,
where applicable the processor, takes appropriate security measures against risks such
as accidental or unauthorised access to, destruction, loss, use, modification or disclo-
sure of personal data’ (Article 7.1). It is completed with a new data breach notification
duty (Article 7.2). The accountability principle appears in the new Article 8bis
(1) which states that Parties must provide that controllers and processors must take all
appropriate measures to comply with the obligations of the Convention and be able to
demonstrate their compliance.

3. Case law

The CJEU ruled in the Bara case\(^4\) that the requirement of fair processing of personal
data mandates that a public administration informs data subjects when it transfers
their personal data to another public administration. The Court has also ruled in
Schecke and Eifert\(^5\) that to be admissible, a legal obligation to process personal data
(in casu to publish personal data on every beneficiary of EU agricultural funds) must
respect the principle of proportionality (which is part of the requirement for a legiti-
mate purpose). The Court has examined the respect for this principle of proportionali-
ty in several cases, one of the most well-known being the Digital Rights Ireland case.\(^6\)
In that case, the Court found that this principle was not respected. It notably stated
that there should be criteria to determine the relevant data as regards the purpose of
the processing, as well as to determine the appropriate time-limit for the data reten-
tion. The Court went even further in the Tele2 Sverige AB case\(^7\) where it stated that
legislation prescribing a general and indiscriminate retention of data exceeds the lim-
its of what is strictly necessary and cannot be considered to be justified.

The European Court of Human Rights (ECtHR) has ruled that processing of personal
data may constitute an interference with the data subject’s right to respect for private
life. To be justified, such an interference must notably be in accordance with the law,
which can be correlated with the requirement for lawful processing. This law must be
foreseeable as to its effects. In the Rotaru case\(^8\), the Court indicated that, to be fore-
seeable, domestic law must lay down limits on the powers of the authorities: the law
must define the type of information that can be processed, the categories of persons
on whom information may be collected, the circumstances in which such measures

\(^4\) Case C-201/14, Bara, at para 34 et seq.
\(^5\) Joined cases C-92/09 and 93/09, Schecke, at paras 86-89.
\(^6\) Joined cases C-293/12 and C5-94/12, Digital Rights Ireland.
\(^7\) Joined cases C-203/15 and C-698/15, Tele2, at para. 107.
\(^8\) ECtHR, Rotaru v. Romania.
may be taken, the persons allowed to access these data and the limits of retention of these data.

Concerning the fairness and transparency principle, the ECtHR considers that the collection and storage of personal information relating to telephone, e-mail and internet usage, without the subject’s knowledge, amounts to an interference with his or her right to respect for private life and correspondence within the meaning of Article 8. The Court has said repeatedly that access to their data must be granted to data subjects. In the M.S. case, the Court added to this transparency requirement the necessity that operations done with personal data (such as communication of the data to a third party) are within the reasonable expectations of the data subject. The Court noted that the further use of the data at stake pursued a different purpose that was beyond the expectations of the applicant and concluded that this amounted to an interference with the applicant’s right to private life.

In the S. and Marper case the Court affirmed that data processing must be proportionate, that is to say appropriate in relation to the legitimate aims pursued and necessary in the sense that there are no other appropriate and less intrusive measures with regard to the interests, rights and freedoms of data subjects or society. Moreover, it should not lead to a disproportionate interference with these individual or collective interests in relation to the benefits expected from the controller. Notably the retention of data must be proportionate in relation to the purpose of collection and must be limited in time. The S. and Marper case was also the opportunity for the Court to expressly mention the requirements of data quality and time limits for the retention of the data: it states that ‘The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored’.

C. Analysis

1. Lawfulness, fairness and transparency principle - Article 5(1)(a)

The first basic requirement regarding data protection is that personal data be ‘processed lawfully, fairly and in a transparent manner in relation to the data subject’.

As in the DPD, data processing must be lawful to the extent that it respects all applicable legal requirements (for example the obligation of professional secrecy if applicable). Article 6 GDPR has been re-titled ‘lawfulness of processing’ rather than ‘Criteria for making data processing legitimate’ as in the DPD, and one may find in this provision the conditions for processing to be lawful. In fact, Article 6 GDPR states that processing shall be lawful only if and to the extent that at least one of the hypotheses it lists applies (see further the analysis of this provision). In the same way, Arti-

---

9 ECtHR, Copland v United Kingdom.
10 ECtHR, Haralambie v. Romania; ECtHR, Gaskin v. United Kingdom.
11 ECtHR, M.S. v. Sweden, para. 35.
12 ECtHR, S. and Marper v. UK.
13 See also ECtHR, Szabo and Vissy v. Hungary.
14 ECtHR, S. and Marper v. UK, para. 103.

de Terwangne
Article 5

Article 8 LED sets out the conditions required for processing to be lawful in this field. Following the comment made by the European Union Agency for Fundamental Rights and the Council of Europe\(^\text{15}\), the principle of lawful processing is also to be understood by reference to conditions for lawful limitations of the right to data protection or of the right to respect for private life in light of Article 52(1) of the EU Charter of Fundamental Rights and of Article 8(2) ECHR. Accordingly, to be considered as lawful, processing of personal data should be in accordance with the law, should pursue a legitimate purpose and be necessary and proportionate in a democratic society in order to achieve this legitimate purpose.

*Fair* processing implies that data have not been obtained nor otherwise processed through unfair means, by deception or without the data subject’s knowledge\(^\text{16}\). For the sake of clarity, the GDPR authors decided to explicitly include the transparency principle with the requirement that data be processed lawfully and fairly, whereas until now commentators had attached the transparency requirement to the notion of fairness\(^\text{17}\).

This *transparency* principle is explained in a long recital (39) which starts by specifying that it ‘should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed’. The recital adds that data subjects should know ‘to what extent the personal data are or will be processed’. It is not clear what is covered by this phrase, which does not correspond to any specific information requirement. Recital 39 goes on to mention the quality of the information to give to data subjects: it should be easily accessible and easy to understand. To this effect, clear and plain language should be used. Moreover, the fairness principle implies that special attention should be paid to the clarity of the language used if addressing information specifically to children. Recital 39 also mentions the content of the information to give in order to be transparent.

Such elements on the quality and content of this information duty are the subject of Articles 12 to 14 dedicated to ‘Transparency and modalities’ (see the discussion of these articles below). Certain details are more connected to the fairness requirement. This is notably the case where recital 39 indicates that natural persons should be made aware of risks and safeguards in relation to the processing of personal data. One does not find such a requirement in the information obligations in Articles 13 and 14. However it is difficult to imagine such a requirement to inform about risks concretely implemented. There is – and this could seem logical – no express transparency requirement in the LED since in most cases systematic transparency would hamper the efficiency of the preventive activity or of the criminal enquiry of public authorities. However, fairness of processing is still required and may imply a certain dose of transparency.\(^\text{18}\)

\(^{15}\) FRA Handbook 2014, p. 64 et seq.

\(^{16}\) See for a case of unfair processing: ECtHR, K.H. and others v. Slovakia.

\(^{17}\) See for example ‘Fair processing means transparency of processing, especially vis-à-vis data subjects.’ in FRA Handbook 2014, p. 76.

\(^{18}\) See also Article 13 LED ‘Information to be made available or given to the data subject’ and Article 14 LED ‘Right of access by the data subject’.

*de Terwangne*
The purpose limitation principle has been regarded for 35 years as the true cornerstone of data protection and a prerequisite for most other fundamental requirements. This principle requires data to be collected for specified, explicit and legitimate purposes (the ‘purpose specification’ dimension)\(^{19}\) and not further processed in a manner that is incompatible with those purposes (the ‘compatible use’ dimension).\(^{20}\) Purposes for processing personal data should be determined from the very beginning, at the time of the collection of the personal data. The processing of personal data for undefined or unlimited purposes is unlawful since it does not enable the scope of the processing to be precisely delimited. The purposes of data processing must also be unambiguous and clearly expressed instead of being kept hidden\(^{21}\). Finally, the purposes must be legitimate, which means that they may not entail a disproportionate interference with the rights, freedoms and interests at stake, in the name of the interests of the data controller.\(^{22}\) ‘What is considered a legitimate purpose depends on the circumstances as the objective is to ensure that a balancing of all rights, freedoms and interests at stake is made in each instance; the right to the protection of personal data on the one hand, and the protection of other rights on the other hand, as, for example, between the interests of the data subject and the interests of the controller or of society.’\(^{23}\) In all cases, data processing serving an unlawful purpose (i.e. contrary to the law) cannot be considered to be based on a legitimate purpose.

The second dimension of the purpose principle implies that the controller may perform on these data all the operations that may be considered as compatible with the initial purposes. This notion of ‘compatible’ processing of data has raised numerous questions in practice. The authors of the GDPR have sought to better mark it out. Article 6(4) offers a series of criteria allowing to determine whether the processing for a purpose other than that for which the personal data have been collected is to be considered as compatible with this initial purpose.\(^{24}\) Account should be taken of the possible link between both purposes, of the context in which the personal data have been collected in particular regarding the relationship between data subjects and the controller, of the nature of the personal data, ordinary or sensitive, of the possible consequences of the intended further processing for data subjects, and of the existence of appropriate safeguards.\(^{25}\)

Another new element of the GDPR is the clarification that processing personal data for a purpose other than that for which it has been collected is allowed in certain circumstances even if this new purpose is not compatible with the first one. As a matter of fact, the original Commission Proposal opened up this possibility very widely. The purpose principle would have been reduced to the bare bones. The Council would have gone even further, which was heavily criticised,\(^{26}\) by proposing to authorise further

---

\(^{19}\) WP29 2013, pp. 11-12.
\(^{20}\) Ibid., p. 12-13
\(^{21}\) Ibid., p. 39.
\(^{22}\) Boulanger et al. 1997.
\(^{23}\) Draft Explanatory Report Convention 108.
\(^{24}\) This list is based on the one elaborated by the WP29, see WP29 2013, p. 40.
\(^{25}\) Art. 6(4) GDPR. See also rec. 50 GDPR.
\(^{26}\) See notably WP29 press release 2015 and WP29 2013, p. 36-37.
ther processing for incompatible purposes if done by the same controller and provided that the controller’s or a third party’s legitimate interests prevail over the data subject’s interests.\textsuperscript{27} The purpose principle would have been well and truly rendered meaningless. The final text has come back to the protective aim of the purpose principle but softens it in the two following cases: if the data subject consents to the new incompatible purpose or if the processing is based on a Union or Member State law.\textsuperscript{28} Article 4(2) LED permits the processing of data by public authorities for the purposes of prevention, investigation or prosecution of criminal offences even if those data were initially collected for a different purpose, but on condition that the controller is authorised to process such personal data in accordance with Union or Member State law and that processing is necessary and proportionate to the new purpose in accordance with Union or Member State law.

Finally, certain re-uses of data are \textit{a priori} considered as compatible provided certain conditions are met\textsuperscript{29}, as previously permitted under the DPD. These are ‘further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes’.\textsuperscript{30} These categories of further processing are slightly narrower than before since the previous ‘historical purpose’ has given place to ‘archiving purposes’ - and only ‘in the public interest’ - and to ‘historical research purposes’. The ‘scientific purpose’ is also reduced to ‘scientific research purposes’. A clarification of these terms is to be found in a recommendation of the Council of Europe which states that processing of data for scientific research purposes aims at providing researchers with information contributing to an understanding of phenomena in varied scientific fields (epidemiology, psychology, economics, sociology, linguistics, political science, criminology, etc.) in view of establishing permanent principles, laws of behaviour or patterns of causality which transcend all the individuals to whom they apply.\textsuperscript{31} The category of data processing for statistical purposes has remained unchanged.\textsuperscript{32} ‘Statistical purpose’ refers to the elaboration of statistical surveys or the production of statistical, aggregated results.\textsuperscript{33} Statistics aim at analysing and characterising mass or collective phenomena in a considered population.\textsuperscript{34} The LED has also introduced the notion of archiving purpose in the public interest but has kept the wording of the DPD and Framework-Decision 2008/977/JAI as regards ‘scientific, statistical or historical’ use. Article 4(3) LED states that processing falling in the scope of this text may include such uses for the purposes of prevention, investigation, detection or prosecution of criminal offences, provided appropriate safeguards for the rights and freedoms of data subjects are put in place.

\textbf{3. Data minimisation principle - Article 5(1)(c)}

As previously under the DPD, processed personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

\textsuperscript{27} This proposal was aimed at facilitating Big Data operations, see Burton et al. 2016, p. 6.
\textsuperscript{28} See the discussion of Art. 6.
\textsuperscript{29} These conditions are developed in Art. 89(1).
\textsuperscript{30} Art. 5(1)(b).
\textsuperscript{31} Draft Explanatory Report Convention 108, p. 3.
\textsuperscript{32} See the detailed regime for processing for statistical purpose in COM Recommendation 1997.
\textsuperscript{33} Ibid., Appendix, point 1.
\textsuperscript{34} Draft Explanatory Report Convention 108, p. 9.
However, under the GDPR personal data must be ‘limited to what is necessary’ instead of being ‘not excessive’ as in the DPD. The LED has however kept the initial wording and Article 4(1)(c) thereof states that data must be ‘not excessive’. This difference in terms should not have an effect on the scope of the data minimisation principle. Recital 39 specifies that it requires, in particular, that personal data should only be processed if the purposes cannot reasonably be fulfilled by other means. Furthermore, this necessity requirement not only refers to the quantity, but also to the quality of personal data. It is thus clear that one may not process an excessively large number of data (asking an employee for his complete medical file to assess his capacity to work, for example). But one may not process a single datum either if this would entail a disproportionate interference in the data subject’s rights and interests (for example, collecting information about private drug consumption from a job applicant). The ‘limited to what is necessary’ criterion also requires ‘ensuring that the period for which the personal data are stored is limited to a strict minimum’ (see the storage limitation principle below).

4. Accuracy principle - Article 5(1)(d)

The requirement that data be accurate and, where necessary, kept up to date was already present in the DPD and in Convention 108, and has been maintained in the GDPR. All inaccurate data should be rectified or erased. The controller must take every reasonable step to ensure respect of this accuracy principle. The GDPR clarifies that this intervention must be done without delay. Article 7(2) LED requires that competent authorities take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. These authorities must, as far as practicable, verify the quality of data before communicating it. Article 7(2) LED goes further in specifically providing in the field of police activity that: ‘As far as possible, in all transmissions of personal data, necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up to date shall be added’.

5. Storage limitation principle - Article 5(1)(e)

This provision represents no real change to the prohibition in the DPD against storing personal data in a form which permits identification of data subjects beyond the time necessary to achieve the purposes of processing. However, there is a new element in recital 39, which invites controllers to establish time limits for erasure or for a periodic review. This will ensure that the personal data are not kept longer than necessary.

Article 4(1)(e) LED provides for the same prohibition and Article 5 LED also mandates that appropriate time limits be established for the erasure of the data or for a periodic review of the need for the storage of the data. The text requires procedural measures to be adopted to ensure that those time limits are observed. Article 25 GDPR and Article 20 LED must be taken into account here since they mandate that controllers implement appropriate technical and organisational measures for ensuring

35 See Ibid. for an explanation of the notion of ‘excessive’ data.
notably that, by default, the legitimate period of storage of personal data be respected. Such measures could be expiry dates determined for each set of data.

Moreover, the storage limitation principle permits the storage of personal data for longer periods if it is for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and is subject to implementation of appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subject.

6. Integrity and confidentiality principle – Article 5(1)(f)

Under the title of ‘integrity and confidentiality’ may be found the crucial requirement of security that is now included in the list of fundamental principles of data protection. Personal data must be processed in a manner that ensures their appropriate security, ‘including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures’. This principle mirrors more or less the terms of Article 17 DPD. A whole section of Chapter IV dedicated to controllers and processors develops this duty of security.\(^\text{36}\) This duty includes, and this is new, the requirement to notify personal data breaches to the supervisory authority and in certain cases to the data subjects too. The LED contains the same articulation of the principle of integrity of data appearing in the list of fundamental protection principles (Article 4(1)(f)) and provisions developing further the security duty in a separate section (Articles 29 to 31).

7. Accountability principle – Article 5(2)

The list of fundamental principles of data protection ends with the statement that the controller shall be responsible for compliance with all the previous principles. A new element is introduced in comparison to the DPD: the controller must now be able to demonstrate that the processing is in compliance with these legal rules.\(^\text{37}\) This requirement not only to ensure but also to be able to demonstrate compliance to GDPR is developed in Article 24 dedicated to the responsibility of the controller (see the discussion of this article below).

---

\(^\text{36}\) See the discussion of Art. 32 to 34.

\(^\text{37}\) WP29 2010.
Select Bibliography

Academic writings


Legislation

COM Recommendation 1997: Committee of Ministers of the Council of Europe, ‘Recommendation concerning the protection of personal data collected and processed for statistical purposes’ (R(97)18, 30 September 1997).


Papers of data protection authorities


Reports


Article 6

Lawfulness of processing

Dr. Waltraut Kotschy

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
   (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
   (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
   (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
   (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
   (e) 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;
   (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
   (a) Union law; or
   (b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

Kotschy
4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
(d) the possible consequences of the intended further processing for data subjects;
(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Relevant recitals

(40) In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

(41) Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the ‘Court of Justice’) and the European Court of Human Rights.

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

(44) Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.

(45) Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal
obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.

(46) The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

(48) Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients’ or employees’ personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.
(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. 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, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.

(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the 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, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

CLOSELY RELATED PROVISIONS

Article 4(11) (definition) (see recital 32), Article 7 (conditions for consent), Article 8 (conditions applicable to child’s consent), Article 9(2) (processing of special categories of personal data) (see recital 51); Article 5
Article 6

(principles relating to processing of personal data) (see too recital 39), Article 23 (restrictions) (see recital 73), Article 89 (safeguards relating to processing for archiving, research and statistical purposes) (see recitals 156-163)

RELATED ARTICLES IN LED [Directive (EU) 2016/680]

Article 4 (data processing principles) (see recital 29), Article 5 (time-limits for storage and review), Article 8 (lawfulness of processing) (see recitals 33 – 35), Article 9 (specific processing conditions) (see recital 36)

RELATED ARTICLES IN EPD [Directive 2002/58/EC]

Article 5 (confidentiality of communications), Article 6 (traffic data), Article 9 (other location data)

RELEVANT CASE LAW

CJEU


ECtHR

A. Rationale and Policy Underpinnings

1. Article 6(1)

The principle of ‘lawful processing’, which is one of several data protection principles under Article 5 GDPR, requires that every processing operation involving personal data must have a legal basis. Article 6(1) stipulates what may constitute such a legal basis. At the same time, it must be kept in mind that legally sound processing of personal data will necessitate fulfilling also all other of the core principles for processing personal data set out by Article 5(1).

The list of legal grounds for processing contained in Article 6(1) must be understood as exhaustive and final – it can neither be supplemented nor otherwise amended by interpretation. As far as Member States’ legislators are, at all, allowed to act under Article 6(1), all legislative activities must keep within the strict boundaries it sets. The elements in the list must be seen to be legally equal. There is no ranking between Article 6(1)(a) to (f) in the sense that one ground has normative priority over the others. However, in the private sector, consent (Article 6(1)(a)) may in practice play a salient role as a potential substitute whenever there is no contractual context, no detailed legal rules about a fitting legal basis, or the scope of ‘legitimate interests of the controller or of a third party’ is particularly difficult to assess. This may also be the reason why it was deemed necessary in the GDPR to define valid consent more extensively than the other legal grounds for processing and - compared to the DPD – to add two articles (Articles 7 and 8) dealing with specific aspects of consenting.

2. Article 6(2)

There is in principle no room for Member State legislation within the remit of an EU regulation, as EU regulations may only be particularised and complemented by additional EU law. Nevertheless, the GDPR explicitly allows Member States to ‘maintain or introduce more specific provisions’ for processing personal data based on Article 6(1) (c) or (e), or in the context of processing situations specifically dealt with in Chapter IX GDPR, which concern, amongst other matters, media, employment relationships, or archiving and research and statistics.

Article 6(2) represents a compromise between the aim of harmonising data protection law throughout the whole Union, which would actually exclude any Member State law in this area, and the fact that more precise rules in the specific areas of application of data protection are advantageous for the legal subjects and cannot be achieved solely by Union law within a reasonable time frame. As harmonisation was felt to be particularly important in the ‘private sector’, empowerment of Member States’ legislators is limited to rules for the public sector (Article 6(1)(e) and to special legal obligations for controllers (Article 6(1)(c)). For processing on grounds of Article 6(1)(f), which is the core of private sector processing, there is no general empowerment for Member States to create data protection rules. Only in those specific areas of processing which are listed in Chapter IX GDPR may Member State legislation maintain existing rules or adopt new rules. In all cases covered by Article 6(2), Member State law maintaining or introducing more specific data protection rules must fully comply with the rules under the GDPR.

---

1 See Arts. 6(2) and (3).
2 Member States were also not permitted to introduce changes or additions to the six grounds for processing personal data under Article 7 DPD (the direct antecedent to Article 6 GDPR).
3 WP29 2014, p. 10
3. Article 6(3)

This provision has two functions, first to clarify that only legal provisions under EU or Member State law – not foreign law - can provide a legal basis for processing based on Article 6(1)(c) or (e); and second, to give guidance as to the appropriate content of such EU or Member State legal provisions.

As to the first purpose of Article 6(3), this problem is particularly acute in times of globalisation, where controllers acting under different legal systems may be confronted with conflicting legal obligations. Article 6(3) confirms the priority of EU data protection law over obligations derived from foreign legal provisions, to which the controller might be subject outside the territorial applicability of the GDPR.

Additionally, Article 6(3) elaborates on those special topics which should be dealt with in provisions (of Union or Member State law) specifying the conditions for processing based on Article 6(1)(c) or (e). It admonishes the legislators to include especially clear statements on the concrete purpose of processing, on the types of data which may be processed for this purpose, on the data subjects, on lawful recipients of data, and, in general, to introduce ‘measures to ensure lawful and fair processing’.

4. Article 6(4)

The purpose limitation principle (set out in Article 5(1)(b)) requires that the purpose of processing shall be defined at the time of collection of the data and prescribes, as a point of departure, that all consecutive processing operations shall not exceed the defined purpose. This rule is specified and enhanced by acknowledging that the scope of ‘one’ defined purpose shall include processing operations which are ‘compatible’ with the initially named purpose.

The concept of ‘compatibility’ is not defined in more detail in Article 5(1)(b) – a shortcoming which is remedied by Article 6(4) which is new in comparison to the DPD. With data sharing and repurposing of personal data becoming increasingly prevalent, as such data are a valuable commodity, more guidance on what may be considered as ‘compatible further use’ was deemed necessary. WP29 released an opinion on the topic of purpose limitation in 2013, which deals extensively also with the concept of ‘compatibility’. The main ideas of this opinion concerning the assessment of ‘compatibility’ are reflected in Article 6(4).

Additionally, Article 6(4) deals with the situation that ‘incompatible further use’ of data might exceptionally be necessary or intended and regulates the conditions for such use. These conditions are logically derived from the fact that incompatible further use is an interference with the principle of purpose limitation and may therefore only take place in compliance with Article 23 GDPR. This latter provision deals with legal restrictions of rights and obligations under – inter alia - Article 5 GDPR, and displaces Article 6 (1) in this respect as the relevant provision for determining the bases of lawful processing.

---

4 WP29 2013.
B. Legal Antecedents

1. EU legislation

Article 6(1) is fully based on and nearly identical to Article 7 DPD. Long experience in applying the latter provisions to the daily practice of information processing, proved that the list they contain is comprehensive and serves well, even under rapidly changing technological-organisational developments. Thus, only minor changes were enacted.

2. International treaties

In 1981 the Council of Europe Convention 108 formulated the principles for lawful processing of personal data for the first time in international law. These principles were taken over into Article 6 DPD and, subsequently, into Article 5 GDPR. The Convention did not, however, formulate a list of concrete legal bases for data processing. Developing an exhaustive list of concrete reasons for lawful data processing is one of the special achievements of EU data protection law.

Even the proposed modernised version of Convention 108 eschews such a list. In Article 5(2), it adopts the formulation chosen in Article 8(2) CFR, mentioning only ‘consent’ and ‘some legitimate basis laid down by law’.

As concerns ‘compatible further use’, this exemption or restriction of the purpose limitation principle was always inherent in Article 5 of Convention 108. The amended proposal for Article 9 of Convention 108 resulted in a provision comparable to Article 23 GDPR. There is, however, no equivalent to Article 6(4).

3. Case law

The CJEU has struck down attempts to modify Article 7 DPD by way of national legal provisions, especially concerning limitations on Article 7(f). With reference to its earlier judgment in ASNEF, the CJEU recently remarked: ‘The Court has held that Article 7 of Directive 95/46 sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as being lawful and that the Member States cannot add new principles relating to the lawfulness of the processing of personal data or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in that article’.

In the Huber case the CJEU interpreted Article 7(e) DPD in the light of the requirement of necessity of processing for the defined purpose(s). Data about the applicant, an Austrian citizen living in Germany, had been entered into a register, which was operated by German authorities on foreigners only, including non-German EU citizens. These data were used by the German authorities to different ends, inter alia to apply the legislation relating to the right of residence, for statistical purposes and for the purposes of fighting crime. There was no comparable database for German nationals. The applicant successfully claimed discrimination. One of the questions put to the court was, whether this central register was compatible with the DPD in so far as the legitimacy of processing personal data depends on

5 Joined Cases C-468/10 and C469/10, ASNEF.
6 Case C582/14, Breyer, at para. 57.
7 Case C-524/06, Huber.
whether it is ‘necessary for the performance of a task carried out in the public interest or in the exercise of official authority’. Whereas processing for the purpose of fighting crime, being outside the remit of the DPD, was not included into the deliberations of the court, the court dealt with the question of ‘necessity of processing’ in the context of the right of residence and use for statistical purposes. The court pointed out that the right of residence of a Union citizen in the territory of a Member State other than his own is not unconditional and may be subject to limitations. Therefore, the processing by a centralised register of personal data in order to apply the legislation relating to the right of residence satisfies the requirement of necessity within the meaning of the DPD provided that only the data necessary for that purpose are processed and that the centralised nature of the register enables that legislation to be more effectively applied. However, the Court took the view that statistics do not necessitate the collection and storage of individualised information as in this case. Such processing of personal data does not therefore satisfy the requirement of necessity within the meaning of the DPD.8

C. Analysis

1. Article 6(1)

1.1 General remarks

Every use of personal data is a potential interference with or a limitation of the right to data protection. The GDPR, which only deals with the use of data in the form of ‘processing by automated means’ and ‘processing in filing systems’,9 names six grounds in Article 6(1) for making processing of personal data lawful. In a concrete case, a controller must be able to demonstrate that at least one of these grounds applies to their processing of personal data.10

The choice of the six grounds mentioned in Article 6(1) may at first sight seem somewhat accidental. However, it corresponds to the general rules for lawful limitations on fundamental rights set out in Article 52(1) CFR and Article 8(2) ECHR. Irrespective of the differences in the respective formulations of the ECHR and the Charter,11 the effect of the corresponding rules in these two legal instruments is to be considered as equivalent in substance, although protection under the Charter may be more extensive than under the ECHR.12 Hence, according to the Charter the right to data protection may be limited only if this is more or less explicitly foreseen in an EU or Member State law, and if the content of that law complies with the condition of foreseeing only such limitations which are necessary and apt to achieve the defined purpose of processing, which can be either a public interest or the protection of the

---

8 Necessity of the central register for purposes of fighting crime was not examined by the Court in the light of the DPD, as it does not cover matters of public security or the activities of the State in areas of criminal law.
9 See Art. 2(1) on the material scope of its application.
10 In light of CJEU jurisprudence concerning Art. 7 DPD, the list of reasons for legitimate processing of personal data cannot be extended by Member State law. It is doubtful even whether this list could be substantially enlarged by Union law, as it must be considered to constitute an exhaustive explication of legitimate interference with the fundamental right to data protection – an explication which has, after all, proved its appropriateness by more than 20 years of intensive application.
11 The text of Art. 8(2) ECHR deals only with interferences by public authorities. However, according to ECtHR jurisprudence state parties to the Convention are under a positive obligation to provide safeguards against private interference. Thus, processing of personal data by private sector controllers has to be included within the scope of data protection, and adequate measures for effective protection of data subjects must be adopted by the state.
12 According to Art. 52(3) CFR, ‘the meaning and scope’ of rights, which are guaranteed under the Charter as well as under the ECHR, ‘shall be the same’ as those laid down by the ECHR, but EU law may foresee a more extensive protection.
Article 6

Kotschy

41

rights and freedoms of others. Additionally, the limitation foreseen needs to be proportional and to respect the essence of the fundamental right to data protection.

The function of Article 6(1) GDPR, seen in relation to Article 52(1) CFR, is to specify in more detail what the terms ‘objectives of general interest (recognized by the Union)’ and ‘necessity to protect the rights and freedoms of others’ mean in the context of data protection.

1.2 The bases for lawful processing:

a) Consent of the data subject

According to Article 6(1)(a) GDPR, processing personal data is lawful if the data subject has allowed for processing in a way which satisfies the conditions for valid consent as defined in Article 4(11) and in Articles 7 and 8 GDPR.13

Article 6(1)(a) is not substantively different from its antecedent, Article 7(a) DPD.14 The requirement that consent be ‘unambiguous’ is now a defining element for valid consent in Article 4(11) and is therefore no longer mentioned in point (a) of the list of reasons for lawful processing.

In addition to the conditions required for valid consent, there are general limits to the use of consent as a legal basis for processing. As allowing for the processing of one’s data involves waiving a fundamental right,15 it seems evident that problems could arise if harmful consequences for the protected individual are the result. The WP29 has stressed that consent is not apt to constitute a legal basis for all sorts of processing: ‘The use of consent “in the right context” is crucial’.16 ‘Where the elements that constitute valid consent are unlikely to be present and where the data subject cannot decide in the absence of social, financial, psychological or other pressure, the element of ‘free’ consenting is not secured.’17 Where refusing consent may lead to serious disadvantages for the data subject, consent cannot be considered to have been freely given and would therefore not be valid.18

As a consequence, WP29 considered that in certain areas the use of consent as a legal basis is usually inappropriate. This relates especially to the exercise of authoritative power, which means e.g. that the requirements under Article 6(1)(e) for lawful processing by public authorities cannot be replaced by asking individuals for consent. This relates also to processing in the context of an employment relationship where the lack of legitimate interest

13 As ‘consent’ is a declaration of intent, its validity depends, moreover, on the general prerequisites for valid declarations of intent under the law, which means that the person declaring his/her intent must be ‘sui iuris’ (i.e. of mature age and with full mental capacity). Art. 8 deals with the validity of ‘under age’ consent (children’s consent) in certain circumstances.
14 Art. 7 (a) DPD stipulated that processing is lawful if ‘the data subject has unambiguously given his consent’.
15 It is interesting to note that, contrary to Art. 8(2) ECHR, Art. 8(2) CFR explicitly refers to ‘consent’ as a possible legal basis for processing personal data. The jurisprudence of the ECtHR pursuant to Art. 8 ECHR shows, however, that waiving the right to data protection through consent can also be acceptable under the ECHR. See e.g. ECtHR, Z v. Finland.
16 WP29 2011, p. 10.
17 Ibid., p. 15.
18 See Ibid., p. 13: ‘[F]ree consent means a voluntary decision, by an individual in possession of all of his faculties, taken in the absence of coercion of any kind, be it social, financial, psychological or other. Any consent given under the threat of non-treatment or lower quality treatment in a medical situation cannot be considered as “free” …’. See also rec. 42: ‘[C]onsent should not be regarded as freely given if the data subject … is unable to refuse or withdraw consent without detriment.’
on the side of the employer/controller (Article 6(1)(f)) cannot in all circumstances be replaced by acquiring consent from employees.\(^{19}\)

Another general limitation on the use of consent as a legal basis for processing may exist in the context of linking up a pre-formulated consent clause with a contract, so that closing the contract automatically results in agreeing to the consent clause. The ‘freeness’ of such decision can be questioned.\(^ {20}\)

b) Contract and pre-contractual relationship

Point (b) has been copied in the GDPR from Article 7 DPD without changes. To the extent that processing data about one’s contractual partner (the data subject) is necessary for the fulfilment of a contract by the other contractual partner (the controller), the latter has a legal basis for their processing operations on these data. This is laid out explicitly in Article 6(1)(b), but can also be derived more generally from the fact that the controller, as a contractual partner, has a legal obligation to fulfil his or her contractual obligations according to general legal principles. Legitimacy of processing for fulfilling a contractual obligation could therefore also be understood as a special case of ‘legal obligations’ and even of ‘legitimate interests of the controller’, which would shorten the exhaustive list of reasons for lawful processing in the GDPR considerably. However, tradition in European data protection law has been that these cases are kept separate and have their specific meaning, as is explained further in the context of analysing Article 6(1)(c) and (f).

As to the scope of what is necessary for the performance of a contract, the question arises whether it covers only processing strictly serving the fulfilment of the contract by the controller or whether it includes events which often come to pass in the context of a contract, such as billing or exercise or defence of legal claims arising from the contract. The phrase ‘performance of a contract’ suggests that it comprises all stages necessary for the fulfilment of what was agreed between the contract partners. The purpose of Article 6(1)(b) is to make the legal instrument of ‘contract’ function also under the aspect of data protection. This requires that Article 6(1)(b) covers all data processing which usually is involved in administering contracts, such as, for instance, processing for billing purposes or processing for defects liability etc.\(^ {21}\) For additional activities, such as enquiries about the creditworthiness of a potential business partner or activities aimed at legal enforcement, Article 6(1)(f) may offer a suitable legal basis.\(^ {22}\)

Contrary to the case where consent is the legal basis for processing, the data subject as a contractual partner cannot freely terminate processing of his/her data based on a contract. Only by terminating the contract will the legal basis for processing (at least partly)\(^ {23}\) be removed. The conditions under which contracting parties are legally able to terminate a contract are defined by civil law. Article 6(1)(b) additionally mentions pre-contractual situations as a possible ground for lawful processing. Processing data to fulfil a request of the data subject in a pre-contractual relationship could be based also on conclusive consent of the data subject or even on the ‘legitimate interest’ of the controller. Mentioning it under Article 6(1)(b) as a separate legal basis makes a difference as to the consequences. The data subject

\(^{19}\) See WP29 2011, pp. 15-16, as well as rec. 43.
\(^{20}\) See the last sentence of rec. 43 and Albrecht and Jotzo 2017, at part 3, no. 40. See also WP29 2016, pp. 8-10.
\(^{21}\) In this sense also Albers 2017, no. 31.
\(^{22}\) See also WP29 2014, p. 18.
\(^{23}\) However, in many cases some data will have to be stored for purposes of documentation.
cannot terminate lawful processing either by withdrawing consent or by objecting.  

Considering how vague the concept of ‘pre-contractual relationship’ is, it might have been better to leave this case with Article 6(1)(a) or (f) in order to provide the data subject with better legal possibilities for interfering with such processing. To secure the right balance, the scope of lawful processing for pre-contractual relationship under Article 6(1)(b) must therefore be considered as strictly limited to what is ‘necessary’ according to general knowledge and practice for complying with the data subject’s request. Processing is only justified as far as the usual expectations of the data subject would go and as far as it is typically adequate for the kind of request which was expressed by the data subject.  

Lawful processing of sensitive data (‘special category’ data in the sense of Article 9 GDPR) in the context of a contract or a pre-contractual relationship is extremely limited. Only in those (few) areas which are explicitly mentioned in Article 9(2) and which are eligible for creating legal obligations under civil law, can a contractual relationship be a legal basis for processing. The most prominent examples are the areas of employment contracts and of contracts for medical treatment. It seems justified to assume that typical pre-contractual situations in these areas would also be covered, such as, for instance, data processing in the stage of being interviewed for employment or of undergoing preparatory organisational measures for medical treatment. Data collected in the course of these situations would, however, have to be deleted without delay as soon as the pre-contractual phase was ended if there exists no further legal basis such as the closing of the contract or consenting.

Underlying point (b) is the assessment that it is justified to process personal data as far as it is necessary to fulfil a contract between the data subject and the controller, because fulfilling a contract is a general obligation under civil law. Following this reasoning, other civil law relationships which create legal obligations on the controller vis-à-vis the data subject should also be acknowledged as a legal basis for processing, as far as processing is necessary for complying with such legal obligations. This would be particularly adequate as point (c) of Article 6(1), referring to ‘legal obligations’, does not apply to legal obligations under civil law, as will be shown in the next paragraph.

c) Processing for compliance with a legal obligation to which the controller is subject

The formulation of Article 6(1)(c) GDPR is identical with the formulation of the corresponding Article 7(c) in the DPD. Article 6(1)(c) deals with such legal obligations which necessitate the processing of data of others, in order to be able to fulfil the obligation; these ‘others’ can be customers, employees, suppliers or others. The purpose of processing needs to be the fulfilling of the obligation. Everyday examples for situations which fall under point (c) would be the processing of data about employees by the employer for social insurance purposes or the processing of data of customers by banking institutions for legal obligations under laws on money laundering.

In general, the source of a legal obligation may vary. The obligation may be directly spelled out in a provision in the law or be the result of an agreement between private parties. The wording of Article 6(1)(c) does not provide clarification as to the type of legal obligations covered. However, this provision is traditionally understood as relating only to such

---

24 Art. 21.
25 WP29 2014 comes to the same conclusion, giving examples on p. 18.
obligations, which originate directly from a provision in the law and not from any intermediary or additional stipulation between private natural or legal persons.\textsuperscript{26}

Article 6(1)(c) would also cover situations where the obligation is not entirely specified in a law but by an additional legal act under public law such as secondary legislation or even ‘by a binding decision of a public authority in a concrete case’.\textsuperscript{27} Whether 6(1)(c) also covers legal obligations of public authorities is questionable as these are also dealt with under Article 6(1)(e). The examples chosen by Dammann and Simitis\textsuperscript{28} to illustrate the scope of Article 7(c) seem to limit its applicability to private sector controllers. By contrast, the WP29 is in favour of including all cases of obligations derived directly from a legal provision under Article 6(1)(c): ‘It could also be an obligation to which a public authority is subject, as nothing limits the application of Article 7(c) to the private or public sector.’\textsuperscript{29} The consequences of such interpretation are not significantly disadvantageous for the data subject. The ‘right to object’ is limited to data processing on the basis of Article 6(1)(e), so evoking Article 6(1)(e) as a legal basis may seem to be better for the data subject at first glance. However, if a public sector controller is subjected to a direct and explicit obligation formulated in a law, the need to clarify the justification of processing by means of objection would arise in fewer cases. Moreover, the data subject can always invoke the right to deletion on grounds that a certain processing operation is unlawful as it does not have a sufficient legal basis. In sum, Article 6(1)(c) covers such processing of personal data as is necessary for fulfilling a concrete obligation derived directly from a legal provision.\textsuperscript{30} Article 6(1)(c) is applicable to private sector controllers as well as public sector controllers.

Legal provisions do not only convey concrete obligations onto legal subjects, they may also authorise or license somebody to do something. Where the authorised controller is a public authority Article 6(1)(e) would be the first choice for dealing with this situation. In the sphere of public law, the legal obligation to act is very often the result of a more general authority being vested with certain competences or tasks. Where an authorisation refers to a private sector controller, Article 6(1)(f) seems to be the best fitting legal basis. A controller who is entitled by law to do something can rely on a ‘legitimate interest’ when he or she chooses to make use of that entitlement. The more concretely the authorisation is formulated, the less controversial the question of possibly overriding the interests of the data subjects will be.

d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person

This basis for lawful processing has been expanded to include ‘vital interests of other natural persons’ as well as of the data subject. Recital 46 describes a ‘vital interest’ as an interest which is ‘essential for the life’ of an individual. Using information on the data subject in order to be able to assist where his/her basic needs such as food, housing, medical care etc., are

\textsuperscript{26} See e.g. WP29 2014, p. 19: ‘For Article 7(c) to apply, the obligation must be imposed by law (and not for instance by a contractual arrangement)’. This scope of applicability can also be traced through the history of this provision. Art. 7(c) of the DPD was the final version of a draft provision which initially contained an explicit reference to ‘obligations imposed by national or EC-law’ as opposed to legal obligations founded in a contract or other private law legal instrument. See the Amended Proposal to Directive 95/46, Explanatory statement to Article 7, as mentioned in Dammann and Simitis 1997, p. 146. See also Frenzel 2017, no. 16.

\textsuperscript{27} WP29 2014, p. 20.

\textsuperscript{28} Dammann and Simitis 1997, p. 150.

\textsuperscript{29} WP29 2014, p. 19. See also Frenzel 2017, no. 18.

\textsuperscript{30} Art. 6(3) confirms explicitly that this must be an obligation under EU or Member State law in order to be relevant.
seriously endangered, seems justified, as the right of the data subject to life\textsuperscript{31} takes precedence over his/her right to data protection. Processing data on grounds of ‘vital interests’ requires that a situation of concrete and imminent danger exists for the data subject.\textsuperscript{32}

A specific problem in this context is the role which the data subject should play in the course of taking the decision to process his or her data on grounds of ‘vital interests’. Contrary to Article 9 GDPR (dealing with special categories of data), Article 6(1)(d) does not mention that the decision to process shall be taken by the controller only if the data subject is incapable of consenting.

The principle of ‘fair processing’ might require, nevertheless, that the data subject should be consulted if possible. On the other hand, there may even exist legal obligations which override the will of the data subject. In such constellations, the legal basis for processing will rather be found in ‘fulfilling legal obligations’ than in acting on behalf of vital interests of the data subject. Recital 46 points in this direction, stating that ‘vital interests’ should be made use of as a legal basis only ‘where the processing cannot be manifestly based on another legal basis’. Article 6(1)(a), (c), (e) or (f) would seem to offer such alternatives.

The reference to ‘vital interests of another natural person’ (i.e., a natural person other than the data subject) in Article 6(1)(d) is a change from Article 7 of the DPD and its significance should be analysed. Survival is a ‘legitimate interest’ pursued by every individual. If a controller processes data of one individual for the purpose of assisting another individual to survive, this is actually a clear case of processing on the basis of Article 6(1)(f). This latter provision contains a perfect balance of interests. As long as processing data for the vital interests of a third person respects proportionality concerning the interference into the rights of the data subject, all legitimate interests which are at stake in such a situation are properly taken care of. However, contrary to Article 7(f) of the DPD, Article 6(1)(f) GDPR is now limited to private sector controllers. This may explain why it was deemed necessary to include a provision on vital interests of third parties which can be made use of by controllers of the public sector.

Understanding processing for the ‘vital interests of another natural person’ as just one case of processing on the basis of Article 6(1)(f) is also important for the correct interpretation of the vital interest clause in Article 9(2)(c),\textsuperscript{33} which could be misunderstood as providing the data subject with the power to decide about life and death of another individual by granting or refusing consent to the processing of his or her data. Irrespective of the formulation of Article 9(2)(c), the last half sentence of this provision must be read as referring only to the case of ‘vital interests of the data subject’. In light of what has been said above on general limits for the applicability of consent, it is inappropriate to consider consent as an apt legal basis for ‘processing for vital interests of third parties’. The moral pressure on the data subject when deciding about the use of his or her data for the survival of another human being would prevent ‘free’ consent, rendering such consent invalid.

\textsuperscript{31} See Art. 2 of the Charter (right to life): ‘1. Everyone has the right to life. 2. No one shall be condemned to the death penalty, or executed’.

\textsuperscript{32} Kramer 2017, no. 23.

\textsuperscript{33} Art. 9(2)(c): ‘processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent’.

\emph{Kotschy}
e) Processing for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

This provision is the general basis for lawful processing of personal data for public sector purposes. Compared to its antecedent in the DPD, Article 6(1)(e) no longer refers to disclosure of data to other controllers in the public sector. This does, however, not result in any substantial changes, as disclosure of data to a public authority by another public authority must be legitimised in the same way as any processing of personal data by an entity which acts in its role as ‘authority’. It must be done ‘for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller’. If the transmission of data to a public authority (or another body subject to Article 6(1)(e)) is performed by a controller who is not subject to Article 6(1)(e), this case will now be treated either as processing under Article 6(1)(c) if such transmission is legally mandatory, or possibly as processing under Article 6(1)(f) if the controller by transmitting data acts within the limits of his or her rights or freedoms as a private law subject. Even Article 6(1)(b) might be applicable if the transfer of data to an authority is necessary to fulfil a contract between the transferring controller and the data subject.

In the English version it is ambiguous whether the words ‘vested in the controller’ relate to ‘exercise of official authority’ or to ‘a task’. The meaning of Article 6(1)(e) is clearer in the German version, where commas are set in order to structure the sentence. Transferring this structure into the English version, it would read as follows: ‘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’. Thus, the reason for processing under Article 6(1)(e) is the fact that it is necessary for a task, which ‘shall be carried out in the public interest or in the exercise of official authority’ and has been ‘entrusted to the controller’. Vesting such a task in a controller requires a legal provision to this effect. Such understanding excludes cases of assignment of ‘tasks’ by contract, even if they were ‘in the public interest’. This will be particularly significant where private entities shall be ‘vested with a task’ in the sense of Article 6(1)(e). Such understanding evidently also underlies the provisions of Article 6(2) and (3) which clearly presume that the obligations under Article 6(1)(c) and the tasks under Article 6(1)(e) are conveyed by provisions in the law.

---

34 Art. 7(e) DPD: Processing is lawful if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.

35 Art. 4(9) contains a definition of ‘recipient’ which seems to exclude public authorities when receiving data in form of an inquiry. The reason for this exemption and its consequences are not clear. If it was meant to result in ‘free data exchange’ with public authorities, it would manifestly infringe the fundamental right to data protection. As ‘a particular inquiry’ must, however, be ‘in accordance with Union or Member State law’ according to Art. 4(9), processing has in the end to fulfil the same requirements as foreseen in Art. 6(1)(e), because every Member State law must be in accordance with the fundamental right to data protection.

36 This is either a private-sector controller or could also be a public-sector controller when renting office space or contracting a processor etc.

37 An example for such a situation would be citizens notifying police authorities about suspected crimes.

38 Art. 6(1) (German version): ‘e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde’.

39 Authorities acting outside of matters of ‘public interest’ or ‘official authority’, e.g. when renting office space, contracting processors etc., will, however, act on the basis of Art. 6(1)(b) or (f).

40 Albrecht and Jotzo 2017, part 3 no. 45, explicitly state, that obligations to process data on the basis of Art. 6 (1)(c) or (e) cannot be the result of private law obligations but only of legal provisions in Union or Member State law enacting public interests. See also Kramer 2017, no. 24: ‘The authority/private entity must have been endowed with the task by a legal provision’. See also: Frenzel 2017, no. 24.
Use of the word ‘or’ in the description of the nature of the tasks, eligible under Article 6 (1)(e), suggests that the remit of this provision is not limited to processing operations of public authorities (in ‘exercise of official authority’) but extends to processing by private bodies. Whether such private bodies would have to be endowed at the same time with official authority in order to qualify for Article 6 (1)(e) is answered controversially. While, for instance, Kramer \(^{41}\) acknowledges only such private entities which are vested with official authority (‘beliehene Unternehmer’) and states that private entities, operating on a commercial basis, although in the public interest, are not covered by Art. 6(1)(e), \(^{42}\) Roßnagel\(^{43}\) does not make such a distinction. Following the text of Article 6 (1)(e), which links the two eligibility criteria by ‘or’ and not by ‘and’, it seems up to the legislators, to decide, when vesting a task of public interest in a private sector controller, whether they want to also attribute ‘authority’ to the controller or not.\(^{44}\)

Processing may be performed on the basis of Article 6(1)(e) if it is necessary for fulfilling the task which was vested in the controller. Necessity to process personal data must be seen in the context of the area regulated by the respective provision within Article 6 (1). Article 6 (1)(e) deals with data protection in the context of the performance of – intrinsically – state or public functions. In this context, processing is necessary as far as it promotes good governance in the sense that it facilitates activities which are in the public interests and are foreseen by law.

The CJEU reflected on ‘necessity’ under Article 6 (1)(e) in Huber.\(^{45}\) In the context of whether a specific centralised register was ‘necessary processing’ the court reasoned as follows: ‘The processing by a centralised register of personal data in order to apply the legislation relating to the right of residence satisfies the requirement of necessity within the meaning of Directive 95/46/EC provided that only the data necessary for that purpose are processed and that the centralised nature of the register enables that legislation to be more effectively applied’. Thus, making the performance more effective can be a criterion for ‘necessity’ in the context of carrying out a task in the public interest or in the exercise of official authority. Moreover, the concept of ‘necessity’ must be interpreted strictly in the light of proportionality: If there are several alternatives to reach a legitimate goal, the one alternative which is least intrusive must be chosen.\(^{46}\)

Contrary to Article 6(1)(c), the assignment of a task as referred to in Article 6(1)(e) will often not result in precisely determined obligations for the controller but rather in a more general authorisation to act as necessary in order to fulfill the task. Concerning the obligation to interpret and weigh interests, Article 6(1)(e) is therefore not so different from Article 6(1)(f). This may also explain why only these two cases under Article 6(1) are eligible for the data subject’s right to object according to Article 21 GDPR.\(^{47}\)

\(^{41}\) Kramer 2017, no. 24. See also Albrecht and Jotzo 2017, p. 73.
\(^{42}\) See Frenzel 2017, no. 23.
\(^{43}\) Roßnagel 2017, no. 11 and seq.
\(^{44}\) This reading of Art. 6(1)(e) evidently also underlies the formulation of Art. 86 GDPR, where the object of ‘public access to documents’ is defined as ‘personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest’. There is no requirement for official authority attributed to the private body in order to qualify under Art. 86.
\(^{45}\) Case C-524/06, Huber, at paras 59-61.
\(^{46}\) Rec. 47. See also Kramer, no. 25. Frenzel 2017, no. 23.
\(^{47}\) In this sense also WP29 2014, p 22
f) Processing on grounds of legitimate interests pursued by the controller or by a third party

A ‘legitimate interest’ is an interest which is visibly, although not necessarily explicitly, recognised by law, more precisely by EU or Member State law. Mere commercial interests will not suffice to establish a ‘legitimate interest’. Particular relevance must be attributed to the fundamental rights recognized in the Charter as they are all potential sources of legitimate interests.48

In contrast to the definition under the DPD, ‘legitimate interest’ in the GDPR refers only to interests of private sector controllers. According to the last sentence of Article 6(1)(f), legitimate interest shall not apply to ‘processing carried out by public authorities in the performance of their tasks’. They are to rely on Article 6(1)(e).

Other differences with Article 7(f) of the Directive is the presence of a new and explicit reference to the interest in special protection of children, and the fact that the legitimate interests of third parties are no longer limited to cases of data transmission.

A ‘legitimate interest’ can be derived from a right49 or from a freedom.50 Both contain the authorisation to act within the limits of the legal boundaries of the right or freedom.51 Whereas ‘rights’ of natural or legal persons52 are usually rather well defined in the law, ‘freedoms’ tend to be less explicit as to their effects and are prone to change in accordance with social developments. Several ‘freedoms’ are, however, formally recognised by law, such as the freedom of expression and information,53 the freedom of arts and sciences,54 or the freedom to conduct a business.55 Examples of ‘legitimate interests’ are given in the recitals to the GDPR. Recital 47 refers to the processing of personal data strictly necessary for the purpose of preventing fraud which would be based on the right to property, or the processing of personal data for direct marketing purposes which relies on the freedom to conduct a business. Both reasons will be the basis for recital 48 which names ‘the transmission of certain data within groups of companies’ as a legitimate interest and for recital 49 which refers to the processing of data for the purposes of ensuring network and information security.56

48 See also Frenzel 2017, no. 28.
49 E.g., from the right to property, according to Art. 17 CFR or the freedom of expression and information according to Art. 11 CFR.
50 Art. 8(2) ECHR mentions ‘rights and freedom of others’ as a possible reason for lawful interference. Fulfilling a legal obligation is certainly also ‘a legitimate interest’ of the person who is subject to the obligation. In EU data protection law, legal obligations are, however, treated traditionally as a separate case under Art. 6 (1).
51 The GDPR does not define the kind of legitimate interests relevant under Art. 6 (1)(f): Any commercial or non-materiel interest will serve, as long as it is legitimate, see Kramer 2017, no. 30. Direct marketing, fighting fraud, data exchange within groups of companies and network security are mentioned as possible examples in rec. 47 to 49.
52 Whereas data protection is only granted to natural persons under the GDPR, Art. 6(1)(f) refers to the rights and freedoms of the controller or of other persons distinct from the data subject (‘third parties’). The controller or the third party may be either a natural or a legal person.
53 Art. 11 CFR.
54 Art. 13 CFR.
55 Art. 16 CFR.
56 A list of examples for legitimate interests which are specifically relevant in practice is given in WP29 2014, p 25.
According to the text of Article 6(1)(f) a controller may process data not only on behalf of his or her own legitimate interests but also because of legitimate interests of third parties. As a controller cannot usurp just anybody’s rights or freedoms and process data based on another person’s legal position, it is evident, that the applicability of this provision can only be very limited. One example is referred to in Article 6(1)(d) where the ‘vital interests of another natural person’ are mentioned as a legal basis for processing. Another possible and not unimportant scenario is the transmission of data to a third party because of legitimate interests of this third party. This situation may occur in particular where a legal provision explicitly entitles or allows a third party to receive data.\textsuperscript{57} However, third parties may also have legitimate interests which are not reflected in specific legal provisions, where such rights or interests cannot be exercised unless a certain (type of) controller takes care of them by collecting and processing data about other persons Article 6(1)(f) might provide a legal basis for processing. The WP29 discusses, for instance, whether interests of a democratic society (this would be the third party) in transparency would justify that someone (this would be the controller) publishes information on the income or remuneration of functionaries (these would be the data subjects).\textsuperscript{58} That such delicate situations should preferably be regulated by law and thus handled under Article 6(1)(c) rather than under Article 6(1)(f) is, however, admitted. If in such a scenario, the data are initially collected for the purpose of responding to the interests of the third parties, there is no ‘further processing’ involved, as the interests of the third parties are the explicitly named reason for data collection. If, however, the necessary data are derived from processing for other initial purposes, the rules of Article 6(4) for ‘further processing’ have to be followed.

All processing for ‘legitimate interests’ is anyway limited to what is plausibly necessary to pursue this interest. In line with the principle of proportionality processing can only be acknowledged as ‘necessary’, if there is no better suited and less intrusive alternative available.\textsuperscript{59} Processing on grounds of Article 6(1)(f) is not allowed where the legitimate interests of the controller or of a third party ‘are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child’.\textsuperscript{60}

A controller, intending to rely on Article 6(1)(f), must therefore perform a special ‘balancing test’, as the WP29 formulates in its opinion.\textsuperscript{61} WP29 offers the following headings for supporting the ‘balancing test’: ‘(a) assessing the controller’s legitimate interest, (b) impact on the data subjects, (c) provisional balance and (d) additional safeguards applied by the controller to prevent any undue impact on the data subjects’.\textsuperscript{62} Adhering to the principle of accountability, this assessment has to be done before starting any processing operations based on Article 6 (1)(f). Further, the assessment needs to be properly documented for being able to demonstrate that the controller’s obligations have been fulfilled.\textsuperscript{63} Processing on

\textsuperscript{57} This is not a case of processing under Art. 6(1)(c), if the controller who initially collected the data is not legally obliged to disclose the data to the third party.
\textsuperscript{58} WP29 2014, p. 27.
\textsuperscript{59} See also Kramer 2017, no. 34. See also: Plath 2018, no. 23.
\textsuperscript{60} The WP29 stresses in its WP29 2014, p. 30, that by the reference to ‘interests or fundamental rights…’ the position of the data subject is protected in a very broad and extensive sense.
\textsuperscript{61} For details see Ibid., p. 33 et seq.
\textsuperscript{62} Ibid., p. 33.
\textsuperscript{63} ‘Following the accountability principle … it should be left to the controller to decide whether he has a legitimate interest to justify certain data processing or whether such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This will be subject to supervision, enforcement and judicial review’, see WP29 2012, p. 13.
grounds of Article 6(1)(f) must, in a pro-active way, explore the likely protection interests of the data subjects and construe a design for the processing operations which avoids infringement of such interests. Recital 47 deals with overriding interests in protection and stresses the importance of the reasonable expectations of the data subjects based on their relationship with the controller. These expectations are actually mentioned as relevant only in Article 6 (4) in the context of further processing. However, recital 47 extends its relevance to Article 6 (1)(f). It suggests that the reasonable expectations of data subjects based on their relationship with the controller should be taken into consideration when deciding whether interests of the data subject ‘override’ the legitimate interests of the controller. Further processing for an incompatible purpose is cited as a particular case of overriding protection interests. Whereas the significance of the data subject’s expectations as a limit for the remit of legitimate interests is fully plausible in the context of further processing, where the data subject was initially not informed about any additional purpose of processing, it seems less convincing outside of further processing. Whether and when a legitimate interest prevails over protection interests or is overridden by protection interests must be judged by common standards, the expectations of the data subjects are relevant only insofar as they go along with these standards as, for instance, with habitual justified use of personal information within a commercial sector. The principle of proportionality will be of utmost importance when balancing legitimate interests in processing data against interests in protecting data from being processed.

1.3. On the relationship between the several grounds of lawful processing

As different consequences are linked to the different points under Article 6(1) it is relevant for controllers to determine how their processing operations fit into the different cases of Article 6(1). Lawful processing can be stopped at the discretion of the data subject only in case of Article 6(1)(a) by means of withdrawing consent. If processing is based on Article 6(1)(f) the controller is obliged to perform a special and documented test of weighing ‘legitimate interests’ in processing against protection interests of the data subject. Article 6(3) requires the existence of a special legal basis if processing shall be based on Article 6(1)(c) or (e). Article 21 grants to the data subject a special ‘right to object’ in case of processing based on Article 6(1)(c) or (f).

Thus, it may be a disadvantage for controllers to rely on consent if they could base their processing on legitimate interests, which cannot be removed at the discretion of the data subject. Undergoing the exercise of weighing legitimate interests against overriding protection interests will be superfluous if processing operations can actually be based on a legal obligation in the sense of Article 6(1)(c). The applicability of the right to object, which results in an obligation of controllers to prove that they did not infringe overriding protection interests, is a further reason why distinguishing correctly between the several cases of Article 6(1) is important.

---

64 The obligation to create privacy protection also by the special design of processing operations is now explicitly foreseen in Art. 25 GDPR.
65 This extended application is followed, for instance, by Kramer 2017, no. 37 et seq.
66 ‘[T]he interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing…’, see rec. 47.
67 On the particular interpretation of ‘reasonable expectations of privacy’ in US jurisprudence, see Feiler et al. 2018, p. 84.
On the other hand, it is no less important to keep in mind that according to Article 52(1) of the Charter the conditions for lawful limitations of the right to data protection ‘apply to all cases of Article 6(1) likewise’. Special conditions for lawful processing mentioned in the several points of Article 6(1) can therefore only refer to *gradual* differences, but never to substantial discrepancies. In the absence of consent, all cases of limitations must be ‘provided for by law’, not only those mentioned especially in Article 6 (3), and proportionality – which is actually ‘a balance’ between the interest in processing and the interest in protection - must be achieved in all cases of processing, even where consent has been given. All cases of Article 6(1) must be interpreted in a way which avoids gaps or discrepancies when compared to the general provisions of Article 52(1) CFR. All legal grounds for lawful processing shall only be used in a way which results in respecting the essence of the right to data protection.

2. **Article 6(2)**

In principle, Member States are not competent to legislate in matters which are subject to an EU Regulation. Exemptions to this rule may, however, be foreseen in Union law. Article 6(2) GDPR contains such an exemption in favour of Member State law concerning legal provisions *specifying and adapting the rules of the GDPR with regard to processing based on Article 6(1)(c) or (e), or concerning the special processing situations listed in Chapter IX of the GDPR*.

This exemption, within its remit, allows for *maintaining* existing Member States’ law, as far as it is compatible with the GDPR, *as well as introducing new legal provisions* under Member State law in compliance with the GDPR. As a result, Member States can actually keep their sector specific data protection law as far as the public sector is concerned, as such law would be based on Article 6(1)(e). The only condition is compliance with the GDPR.

Concerning the private sector, it must be stressed that point (f) is not mentioned in Article 6(2). However, as far as Member State law creates obligations for private sector controllers which *necessitate the processing of personal data*, or deal with ‘specific processing situations’ which are according to provisions in Chapter IX GDPR open for Member States’ legislation, it may also ‘determine more precisely specific requirements for the processing and other measures to ensure lawful and fair processing’ in the private sector.

It remains to be seen, how these competences of the national legislators comply with the overall purpose of the GDPR to ensure a consistent and high level of protection throughout the entire territorial scope of application of the GDPR. As to the content of Member State laws specifying and adapting the rules of the GDPR in cases of processing under Article 6(1)(c) or (e), paragraph 3 of Article 6 contains more detailed rules.

---

68 When WP29 2014 explains on p. 9 that contrary to Art. 6(1)(f) the other cases of Art. 6 (1) are ‘considered as *a priori* legitimate’, that must not be misunderstood. Especially relying on point (e) will very often also require a ‘specific test’ for assuring that a concrete use of personal data for public interests is proportionate.

69 See the deliberations on the limits of consent in the part of this analysis dealing with Art. 6 (1)(a).

70 Rec. 8 mentions in this respect that Member State law may even ‘incorporate elements of this Regulation into their national law’, ‘as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply’.

71 As ‘legitimate interests’ are, however, derived from the body of law to which the controller (or the third party) is subject. Member State law is relevant also in the context of Art. 6(1)(f). Thus, Member State law may contain provisions which create or modify ‘legitimate interests’, but Member State law may not set up conditions for lawful processing based on ‘legitimate interest’. See also Joined Cases C-468/10 and C469/10 *ASNEF* and Case C-582/14, *Breyer*. **Kotschy**
3. Article 6(3)

Article 6(3) clarifies that processing of personal data can be based on Article 6(1)(c) or (e) only if the controller’s obligation, or the task vested in the controller (which necessitate the processing of personal data) are laid down either in Union law or Member State law to which the controller is subject. It follows that obligations or tasks under foreign law cannot provide a legal basis for processing.

The rest of Article 6(3) deals with the nature and content of the provisions in EU or Member state law which are relevant under Article 6(2). The GDPR ‘does not require a specific law for each individual processing. A law as a basis for several processing operations … may be sufficient’. On the other hand, there may be one law conveying a task of public interest to a controller and several additional laws dealing with processing operations which are necessary for different purposes under this task.

Apart from the important question of determining the purpose of processing, examples for such added content of legal provisions under paragraph (2 and) 3 are given in the third sentence of Article 6 (3), or even better (because more comprehensive) in recital 45.

Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing.

Recital 93 mentions, in particular, that laws which delegate tasks to be carried out in the public interest or in the exercise of official authority, might also foresee that an impact assessment has to be done before processing activities are started.

4. Article 6(4)

Article 6(4) GDPR is intended to clarify the concept of ‘compatible further processing’ and to define the conditions for lawful further processing in case of incompatibility.

4.1 The concept of ‘compatible further processing’

Correctly assessing ‘compatibility’ of further use of data is highly relevant as only compatible further use (processing) of data does not require an additional legal basis. The legal basis for the initial purpose of processing is extended to compatible further processing.

Article 6(4) provides tools for the assessment of compatibility by means of a not exhaustive list of items which are important to consider in a concrete case. Two main questions emerge.

---

72 Rec. 45.
73 Such additional laws would be subject to Art. 6(2).
74 Rec. 45.
75 ‘In such a case, no legal basis separate from that which allowed the collection of the personal data is required’, see rec. 50.
in the items listed in Article 6(4)(a) to (e). First, it is difficult to determine the relationship between the initial and the ‘further’ purpose. ‘Compatibility’ of further processing does not require that the new additional purpose of processing is just a ‘sub-purpose’ of the initial purpose of processing. Compatibility of purposes exists also where the new purpose is different but correlates to the initial purpose in the sense that these purposes usually are pursued ‘together’ in close vicinity in a timely as well as a contextual sense, or that the further purpose is the logical consequence of the initial purpose. Recital 50 details ‘the reasonable expectations of data subjects based on their relationship with the controller as to their further use’. This illustrates that compatibility of purposes depends to a high degree on what is usual and what is to be expected in certain circumstances. Using data collected in the course of selling goods to a customer for mandating a carrier to forward the goods to the customer would constitute a ‘compatible further use’. The case of a customer receiving marketing information from an enterprise where he or she had bought goods or services recently is another possible example for ‘compatible further use of customer data’, as customer relationship management (‘CRM’) is a usual activity within a customer relationship in which the data have been originally collected. In such cases the transmission of data to certain recipients will be compatible further processing, if such transmission is necessary to complete the initial purpose of processing. An important and far-reaching example for compatibility is explicitly set out in Article 5(1)(b) GDPR. Further processing for purposes of archiving in the public interest, for scientific or historical research purposes or for statistical purposes shall always be considered as compatible with any other initial purpose of processing.

Second, it is necessary to consider, the extra risks for the data subjects resulting from further processing. The items listed as relevant in Article 6(4)(c) to (e) refer to the necessity of an additional risk assessment concerning the intended further processing and convey the idea that the concept of ‘compatibility’ contains also an element of risk containment. Further processing must not result in a substantively higher risk than the initial lawful processing if it shall qualify as ‘compatible’. This will particularly limit ‘compatible’ further processing of special category data which are mentioned in Article 6(4)(c) as a risk factor. Relying on compatibility cannot extend lawful processing of such data beyond the reasons explicitly listed in Articles 9 and 10. Risks may be mitigated by special safeguards. Data minimisation might be advantageous. Encryption (of the whole data set) is mentioned in Article 6(4)(e) as one example. Pseudonymisation (this is encryption of the identification data) is a second

---

76 This list was modelled according to the deliberations of WP29, put forward in WP29 2013; see also the deliberations of Frenzel 2017, no. 48 et seq.

77 WP29 2013 states on p. 21 that further processing for a different purpose does not necessarily mean that it is incompatible, ‘compatibility needs to be assessed on a case-by-case basis’.

78 See also Kramer 2017, no. 53.

79 In this context the information given to the data subject at the time of the collection of data can be relevant for what are ‘reasonable expectations’.

80 It is only a possible example because additional requirements must be fulfilled in order to qualify as ‘compatible further use’ according to Art. 6 (4).

81 Using customer data for keeping up and enhancing an existing customer relationship is essentially different from using customer data for marketing purposes of a third party – this would never qualify as compatible further use. Support for the assessment of CRM as possibly compatible further use of data can be found in the provisions of the e-privacy Directive on unsolicited mail.

82 Disclosing a file on the use of public grants to official auditors would be an example for compatible further use founded on the logic of grant procedures. Several highly illustrative examples are given in Annex 4 (Practical examples to illustrate the compatibility assessment) to WP29 2013.

83 See Arts. 9 and 10.

84 ‘In general, the more sensitive the information involved, the narrower the scope for compatible use would be’, see WP29 2013, p 25.
example given in (e) for appropriate safeguards. As concerning the special purposes explicitly declared as compatible by Article 5(1)(b), risk containment has to be achieved according to Article 89(1) GDPR. This provision requires adequate technical and organisational measures for ensuring appropriate safeguards, pseudonymisation or even anonymisation being a mandatory measure as far as the ‘purpose of further processing can be fulfilled in that manner’. Additionally, legal measures could qualify for risk containment. Stipulations with recipients of data about limitations of their use and about special data security measures are well established tools to enhance protection and thus lower risks.

If controllers rely on compatibility of further processing they must be able to demonstrate that a compatibility assessment of all relevant circumstances was done and that, in particular, the key factors explicitly mentioned in Article 6(4) have been appropriately dealt with. This applies to the correlation of purposes as well as to the avoidance of additional risks for the data subjects. The formulation of Article 6(4) does not indicate that it suffices to just provide a very high standard of risk containment in order to be able to profit from the privileges of compatible further processing. Even if the data were pseudonymised and all other feasible measures for enhancing protection were in place, ‘compatibility’ would require additionally that the purpose of further processing sufficiently correlates with the initial purpose. Only as far as archiving, research and statistics are concerned, compatibility is focused on risk containment as Article 5(1)(b) GDPR contains a presumption of correlation of purposes.

4.2 On the legal conditions for incompatible further processing

The introductory half-sentences of Article 6(4) regulate quasi ‘en passant’ how controllers ought to proceed if a case of further processing cannot be considered as compatible with the initial purpose of processing. Where there is no special provision in EU or Member State law allowing for the intended kind of (incompatible) further processing, the controller must obtain the data subjects’ consent if he or she wants to pursue this additional purpose.

It should be specifically noted that Article 6(4) does not refer to Article 6(1) for acquiring a legal basis for further processing. ‘Incompatible further processing’ is an interference with the principle of purpose limitation; therefore, not Article 6(1), but only Article 23 GDPR applies, which deals with lawful restrictions of, inter alia, Article 5 GDPR, where the purpose limitation principle is laid down.

According to Article 23 only a special legal provision can be a valid legal basis for interfering with the purpose limitation principle. For the EU or Member State legislators, Article 23 spells out the prerequisites and conditions which such a law ought to fulfil. While Article 6(4) refers alternatively to such legal provisions or consent of the data subjects as a valid legal basis for incompatible further processing, it must be stated that Article 23 does not mention consent. The fact that consent is in spite of non-applicability of Article 6(1) and in spite of lack of any reference to consent in Article 23 explicitly named as a legal basis for incompatible further processing in Article 6(4), must be accepted as acknowledgment of the

85 Such special purposes can be archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
86 The WP29 explained the rationale of such legal assessment in relation to the DPD as follows, ‘Processing of personal data in a way incompatible with the purposes specified at collection is against the law and therefore prohibited. The data controller cannot legitimise incompatible further processing by simply relying on a new legal ground in Article 7. The purpose limitation principle can only be restricted subject to the conditions set forth in Article 13 of the Directive’, see WP29 2013.
legal possibility for data subjects to waive a fundamental right. This is at least concerning the right to data protection in principle always possible and legally relevant.

4.3 ‘Legitimate interest’ in the context of ‘further processing’

Recital 47 states that ‘The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding’. The latter could especially be the case ‘where personal data are processed in circumstances where data subjects do not reasonably expect further processing’.

This reasoning confirms that further processing cannot be made lawful by ‘legitimate interest’ unless it is a case of ‘compatible further processing’. For incompatible further processing ‘legitimate interest’ can never act as a legal basis.

The same is true for the recipient controller if ‘further processing’ involves disclosure of data to a third party: in case of incompatible further use the consent of the data subject or the legal provision being the basis for disclosure must explicitly include disclosure to the recipient.
Select Bibliography

Academic writings

Albrecht and Jotzo 2017: Albrecht and Jotzo, Das neue Datenschutzrecht der EU (Verlag Nomos 2017).


Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis (Nomos Verlag 2017)


Papers of data protection authorities


Article 17

Right to erasure (‘right to be forgotten’)

Dr. 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 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

Kranenborg
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 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing), Article 21 (right to object) (see also recitals 69 and 70)

RELATED ARTICLES IN LED [DIRECTIVE (EU) 2016/680]

Article 16 (right to rectification or erasure of personal data and restriction of processing) (see also recitals 47, 48 and 49)

RELATED ARTICLES IN EPD [DIRECTIVE 2002/58/EC, AS AMENDED]

Article 6(1) (traffic data)

RELEVANT CASE LAW

CJEU

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

Opinion by 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).


C-507/17, Google Inc. v Commission nationale de l’informatique et des libertés (CNIL) (pending).
ECtHR

A. Rationale and Policy Underpinnings

The right to be forgotten in Article 17 was presented as one of the novelties of the GDPR and was used 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 recognizes its increased importance in today’s society, in which personal data is 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 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 Antecedents

1. EU legislation

The right to erasure was also contained in the DPD in the provision on the right of access, Article 12. 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 Treaties

The right to erasure can be found in Article 8(c) of Convention 108. The right to erasure remains unchanged in the draft revised Convention 108 (see Article 8), there is no additional reference to the right to be forgotten as in Article 17 GDPR.

3. National legislation

The right to erasure does not apply, amongst others, if the processing is necessary for exercising the right to freedom of expression and information. The scope of this exception depends 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 leading ruling of the CJEU on the right to be forgotten is the *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 was based on the provisions of the DPD and will be further discussed below.¹

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 take certain 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’.² 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.³

The closest the European Court of Human Rights has come to discussing a ‘right to be forgotten’ was 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 had to reconcile the freedom of expression, in particular freedom of the press, with the right to privacy of the applicant. Building on its well-established case law on conflicts between Article 8 and 10 ECHR, 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.⁴

C. Analysis

The right to be forgotten has 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 current 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.

* The views expressed are solely those of the author and do not necessarily reflect those of the European Commission.
¹ At the moment of writing, several questions were put to the CJEU by the French *Conseil d'État* asking for a clarification of the right to be forgotten with regard to the responsibility of search engines in case of processing of special categories of data (reference registered under Case C-136/17).
² EC Press Release Manni, p 1.
³ Case C-398/15, *Salvatore Manni*, at para. 60.
⁴ See ECtHR, *Węgrzynowski and Smolczewski v. Poland*, at paras. 65 and 66.
Strictly speaking, however, the *Google Spain* ruling did not deal with the right to be forgotten. It concerned the possibility to find a public document by searching the Internet on the individual’s name. In the *Google Spain* case, the outcome was that the document should no longer show up in the list of results produced by the search engine when searching on the applicant’s name. However, the document itself – an article published in a Spanish newspaper – remained publicly accessible. Still, the impossibility of finding the document by searching on the data subject’s name, clearly reduces the ‘public impact’ of the publication on the data subject. The information about the person is not really ‘forgotten’, but removed from the ‘active memory’ of the Internet.

Whether the right to be forgotten could also relate to the removal of the information from the internet as such, is 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 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.¹

The ruling of the ECtHR in the *Węgrzynowski and Smolczewski v. Poland* steps into this lacuna.² It follows from that ruling that when the freedom of the press is at stake, it is not easy to invoke the right to be forgotten. The ECtHR concluded that even if it was found that a publication about a person was incorrect or unlawful, the publication should still remain available, albeit that a right balance with the interests of the person concerned was found by adding a comment to the article on the website informing the public of the outcome of the court proceedings. The ECtHR takes into account the risk that deleting the article from the public domain could amount to rewriting history.

The main challenge regarding the right to be forgotten is thus its relation with freedom of expression. In *Węgrzynowski and Smolczewski v. Poland*, the ECtHR applies its well-established case law on the conflict between Article 8 and 10 ECHR. In the *Google Spain* case the CJEU did not expend many words on the freedom of expression as such.³ When it put all interests at stake in the balance, the CJEU referred to 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.⁴ The interest of the newspaper itself in having wider accessibility of its website was not taken into account. The role of Google as an instrument of freedom of expression in that respect was not directly acknowledged by the CJEU.⁵ That being said, when giving guidance as to what elements should be taken into account when striking the balance, the CJEU referred to elements which seem to be directly taken from the case law of the ECtHR on Article 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 circumstances the right of the general public might prevail. According to the CJEU, this depends on the nature of the information in question, its

---

¹ Case C-131/12, *Google Spain*, at para. 88. See on the liability of a news website for comments on its articles posted by third persons, ECtHR, *Delfi AS v. Estonia*, at para. 140 and further.
² On the right to be forgotten and the ECtHR, see Wechsler 2015.
³ See for criticism on this point Frantziou 2014, Kuner 2015, Kulk and Zuiderveen Borgesius 2015.
⁴ Case C-131/12, *Google Spain*, at para. 81.
⁵ The Court does point at 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 *Ibid.*, at paras. 80 and 87. See for criticism on this point Hijmans 2014.
sensitivity for the data subject’s private life and on 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.\footnote{Case C-131/12, *Google Spain*, at paras. 81 and 97. See on this also Kranenborg 2015, pp. 77-79.}

The CJEU ruling in *Google Spain* has been criticised for leaving the balance of the interests to the search engine provider as data controller. Advocate General Jääskinen in his opinion had warned against it. He stated that internet search engine service providers should not be saddled with such an obligation. According to the AG it would entail an interference with the freedom of expression of the publisher of the web page, who would not enjoy adequate legal protection in such a situation, any unregulated ‘notice and take down procedure’ being a private matter between the data subject and the search engine service provider. It would amount to the censuring of his published content by a private party.\footnote{Case C-131/12, *Google Spain* (AG Opinion), at para. 134. See for an elaborate comparison of the opinion of the AG and the CJEU ruling Allen 2015.} This position was echoed in academic literature.\footnote{See e.g. Spiecker 2015, p. 1053.}

In order to help Google and other search engines to organise compliance with the CJEU ruling, the Article 29 Working Party issued guidelines on the implementation of the ruling.\footnote{See WP29 2014. It is to be noted that the Article 29 Working Party in an opinion of 2008 on search engines had taken the view that a search engine provider was generally not to be held primarily responsible under European data protection law, see WP29 2008, p. 23.} When it turned out that Google was de-listing persons from search results only when the search was performed from Google websites with EU domains, the Article 29 Working Party sent a letter to Google, warning that the decision of de-listing must guarantee the effective and complete protection of data protection rights and that EU law cannot be circumvented.\footnote{See WP29 Letter Google Spain. See also Kranenborg 2015, pp. 76-77. The French Conseil d’État put a question to the CJEU asking for a clarification on the territorial scope of the right to be forgotten. The case was still pending at the moment of writing, see Case C-507/17, *Google Inc*. See also Van Calster 2018.}

As indicated, Article 17(3)(a) and Article 85 GDPR leave it to the Member States to reconcile the right to protection of personal data with the right to freedom of expression and information.\footnote{See the discussion of Art. 85.}

Meanwhile, the right to erasure or to be forgotten is not only relevant in relation to freedom of expression. It can be invoked against any controller who processes personal data, if one of the grounds listed in Article 17(1) GDPR applies. The different grounds partly overlap. If the personal data are no longer necessary for the purpose for which they were collected or otherwise processed (subparagraph a), or consent is withdrawn (subparagraph b), 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.

The three other grounds do not as such assume an unlawful data processing. Article 17(1)(c) lets the right to erasure follow an invocation of the right to object in Article 21 GDPR.\footnote{See the discussion of Art. 21.} In the GDPR the burden of proof following an objection has switched; instead of the data subject, the data controller has to demonstrate compelling legitimate grounds for processing the data.
Such processing should have been based on Article 6(1)(e) or (f) GDPR. If the controller fails to do so, the data have to be erased. In case of direct marketing, the controller has to erase the data upon a simple objection of the data subject. In the situation of personal data processing of a child in relation to the offer of information society services based on the child’s consent, the data have to be erased upon simple request. It follows from recital 65 that the data subject should be able to exercise that right notwithstanding the fact that he or she no longer is a child. It is emphasised that the right to erasure 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 last ground to require erasure (Article 17(1)(e)) is if erasure is legally required in Union or Member State law.

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 processing necessary for exercising the right of freedom of expression and information (subparagraph a) was discussed above. Other situations 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. The right to erasure does not apply either in cases in which the processing is necessary for certain grounds provided for in Article 9, the provision on the processing of special categories of personal data (subparagraph c). 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 (subparagraph d). It is added that this exception can be invoked in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing. The last situation in which the right does not apply is in case of processing necessary for the establishment, exercise or defence of legal claims (subparagraph e).

An example of a legal obligation in Article 17(3)(b) is provided in the Manni ruling. In this case, the question was whether the right to erasure could be invoked with regard to certain personal data (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). After reaching a positive conclusion on this, the CJEU considered that the Member States could not guarantee that the natural persons have the right to obtain, as a matter of principle, after a certain period of time, erasure of the personal data concerning them. According to the CJEU this did not result in a disproportionate interference with the rights of the individuals as laid down in Article 7 and 8 of the Charter. 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. In such situations...
circumstances the right to erasure does not result in the actual deletion of the personal data, but rather takes the data from the public domain.

Once the right to erasure or to be forgotten is successfully invoked, and none of the situations in the third paragraph apply, the controller, if he or she has made the personal data public, is obliged to inform the controllers who are processing such personal data to erase any links to, or copies or replications of those personal data (see Article 17(2)). In doing so, the controller has to 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. 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.22

22 See Art. 17(2) GDPR Proposal.
Select Bibliography

Legislation


Academic writings


Papers of data protection authorities


Others

Article 20

The Right to Data Portability

Dr. Orla Lynskey

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

   (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
   (b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Relevant recitals

(68) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive
the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

(73) Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(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 organizational 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 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.

**Closely Related Provisions**

Art 4(11) (definition of consent); Art 6(1)(a), (b) and (e) (lawfulness of personal data processing) (see too recitals 40, 44 and 45); Art 7 (conditions for consent) (see also recitals 32; 42 and 43); Art 9(2)(a) (consent for processing of special categories of personal data) (see also recital 51); Articles 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject) (see too recitals 39 and 60); Article 13 (information to be provided when the personal data are collected from the data subject) (see too recitals 61 and 62); Article 15 (right of access by the data subject) (see also recitals 63 and 64); Article 16 (right to rectification) (see too recital 65); Article 17 (right to erasure – ‘right to be forgotten’) (see also recitals 65 and 66); Article 18 (right to restriction of processing) (see recital 67); Article 18 (notification obligation regarding rectification or erasure of personal data or restriction of processing); Article 21 (right to object) (see also recitals 69 and 70); Article 22 (Automated individual decision-making, including profiling) (see too recitals 71 and 72); Article 23 (Restrictions) (see further recital 73)

**Related Articles in LED [Directive (EU) 2016/680]**

Article 12 (Communication and modalities for exercising the rights of the data subject) (see also recitals 40 and 46); Article 13 (Information to be made available or given to the data subject) (see further recital 42); Article 14 (right of access by the data subject) and Article 15 (limitations to the right of access) (see also recitals 43, 44 and 45); Article 16 (right to rectification or erasure of personal data and restriction of processing) (see also recital 47); Article 17 (exercise of rights by the data subject and verification by the supervisory authority) (see also recital 48); Article 18 (rights of the data subject in criminal investigations and proceedings) (see too recital 49)

**Relevant Case Law**

**CJEU**

A. Rationale and Policy Underpinnings

A number of distinct yet inter-connected rationales are said to underpin the right to data portability. These range from the rights-based rationale to enhance informational self-determination and empower data subjects to the more economic rationale of reducing switching costs for consumers and promoting competition by potentially lowering barriers to entry to digital markets and encouraging the development of new products and services. Data portability may also enhance the free flow of personal data in keeping with the market integration objectives of EU data protection regulation. For instance, in its 2015 Digital Single Market Strategy for Europe, the Commission suggested that a lack of interoperability and portability between digital services acts as a barrier to the cross-border flow of data and to the development of new services.1

During the legislative process, the UK expressed a reservation in the Council that data portability should not be within the scope of data protection law but rather consumer or competition law and recommended that the provision should therefore be deleted. Other Member States (in particular, Denmark, Germany, France, Ireland, the Netherlands, Poland and Sweden) raised similar concerns regarding the nature and scope of the right to data portability.2 This objective of promoting competition has been noted in several policy documents. For instance, the Article 29 Working Party (WP29) acknowledges that data portability is ‘expected to foster opportunities for innovation’3 while in its ‘Questions and Answers’ on data protection reform, the Commission notes that providing individuals with more control over their personal data through data portability will benefit business as ‘[s]tart-ups and smaller companies will be able to access data markets dominated by digital giants and attract more consumers with privacy-friendly solutions’.4 Commentators on data portability, such as Graef, have suggested that lock-in in online social networks, such as Facebook, may be preventing users from switching despite fierce opposition to privacy policy changes by users.5 Data portability may reduce the risk of lock-in by lowering the costs of switching services for data subjects.

Yet, the role of competition as an objective for data portability, as well as the relationship between the human rights orientated and economic rationales for data portability, remains contested. This is evidenced by the guidelines of the WP29 on data portability. In the initial draft of these guidelines, the WP29 stated that: ‘the primary aim of data portability is to facilitate switching, from one service provider to another, thus enhancing competition between services’ and that it enables ‘the creation of new services in the context of the digital single market strategy’.6 The final draft of the guidelines deletes this sentence and highlights that data portability ‘aims to empower data subjects regarding their own personal data, as it facilitates their ability to move, copy or transmit personal data easily from one IT environment to another’.7 To emphasize this point it

---

2 Council Interinstituitorial File Portability, p 3.
3 WP29 2017, p.5.
4 EC Factsheet 2015.
5 Graef 2015, p.506.
6 WP29 2017, p.4.
7 Ibid.
states that whilst ‘the right to data portability may enhance competition between services (by facilitating service switching), the GDPR is regulating personal data and not competition.’

Thus, it will likely be for the European Data Protection Board (EDPB), in the first instance, and later perhaps the Court of Justice to clarify which of the underpinning rationales for data portability should prevail in case of conflict.

B. Legal Antecedents

1. EU Legislation and International Treaties

There is no legal antecedent for data portability in the EU and data portability has thus been classified as a ‘brand new right’. The right has been linked within the data protection regime to the data subject’s right of access to personal data. The European Parliament rapporteur suggested, on first reading, that the right to data portability should be merged with the right of access, in Article 15 GDPR. The data portability would then strengthen the right of access. Ultimately however the Council resisted the merger of the two rights. Nevertheless, parts of the doctrine view data portability as an extension of the right of access, and that portability should be ‘modulated in practice’ to mirror the right of access in some ways (for instance, to allow the data subject to select what should be transferred and the data controller to distinguish between categories of personal data). However, the right to data portability is narrower in scope than the right of access (for example, it only applies to personal data ‘provided by’ the data subject) while others suggest that the right to data portability – at least as described in the WP29 guidelines – is ‘something much more radical’ than the existing right of access.

Data portability may have been inspired by the concept of number portability, introduced by the EU’s Universal Service Directive, which entitles consumers to switch from one mobile phone provider to another while retaining their mobile phone number. The GDPR impact assessment notes that portability is ‘a key factor for effective competition, as evidenced in other market sectors, e.g. number portability in the telecom sector’ while the European Data Protection Supervisor (EDPS) notes that data portability would allow ‘users to transfer between online services in a similar way that users of telephone services may change providers but keep their telephone numbers’.

The right to data portability has, thus far, also been absent from international treaties although a right to access personal data is set out in several treaties. For instance, Council of Europe Convention No 108 provides for a right of access in Article 8(b) which provides that ‘any person shall be enabled to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are

---

8 Ibid.
9 Scudiero 2017, p. 119. See also CIPL 2017, p.1.
10 Vanberg and Ünver 2017, p.2.
11 Recital 63 facilitates this in the context of the access right. See also CIPL 2017, p.3.
12 Cormack 2017.
13 Art. 30 Universal Services Directive.
15 EDPS 2014, p.15.
stored in the automated data file as well as communication to him of such data in an intelligible form’.

2. National legislation

The Philippines is the only non-EU state, to date, to enact a general right to data portability as part of its domestic data protection legislation. In 2012, it signed into law a data protection act and implementing legislation. The 2012 Act sets out a right that is broader than the GDPR right as it does not require that the personal data should be ‘provided by the data subject’. However, this broad right is qualified by the accompanying implementing rules which state that the exercise of the right shall ‘primarily take into account the right of data subject to have control over his or her personal data being processed based on consent or contract, for commercial purpose, or through automated means’. These qualifications were likely introduced in order to align the right to its GDPR equivalent. While the right was part of a 2012 Act, the final version of the ‘Implementing Rules and Regulations’ that accompany the 2012 Act were adopted only in August 2016. There is therefore no decisional practice to draw upon yet.

A sector-specific right to data portability exists in the United States for medical data. Patients can access and obtain a copy of their data pursuant to the 1996 Health Insurance Portability and Accountability Act (HIPAA). The rights of patients to, amongst other things, access, correct and obtain a copy of their medical records from public and private healthcare providers was initially enacted to improve the efficiency and effectiveness of the healthcare system. However, the right of individuals to ‘get it, check it, use it’ is now regarded as a consumer empowerment tool, and enforced by the US Office for Civil Rights.

Voluntary sector-specific initiatives exist at national level in the United States and the United Kingdom. In the United States, the Obama administration introduced a series of ‘My Data’ schemes in 2010 with the aim of enabling consumers to access their own personal data in certain sectors. For example, the ‘Green Button’ scheme enabled consumers to access their electricity utility data while the ‘Get Transcript’ scheme allowed individuals to access the tax data held by the Internal Revenue Service about them. The White House Office of Science and Technology Policy launched a consultation in 2016 to ascertain whether a broader right to data portability – more akin to that set out in the GDPR –would be desirable. This consultation concluded that although a more general data portability scheme might be incentivized, it should not be mandated.

---

16 Philippine Data Privacy Act 2012, section 18.
17 Ibid., section 36.
18 Hunton & Williams 2016.
19 See HIPAA Preamble.
In the UK, the Government eschewed legislation to mandate data portability and instead took a power pursuant to the Enterprise and Regulatory Reform Act 2013. Data portability is therefore operating on a voluntary basis, but the Secretary of State can introduce regulations to make it compulsory should the government be unsatisfied with the progress made on a voluntary basis. The ‘midata’ initiative introduced in 2011 was part of a wider consumer empowerment strategy and it sought to give individuals access to electronic data regarding their transactions in a machine-readable and portable format. Such transaction data would exclude personal data regarding transactions made using an unregistered guest account, or other complaints or communications data held by companies. The midata scheme was also only focused on three sectors: namely, the financial sector, energy supply and the mobile phone sector. Thus, like the US ‘My Data’ schemes, the UK midata initiative is more limited in scope and application than the GDPR right.

3. Case law

Given that there is no predecessor to the right to data portability in the 1995 Data Protection Directive, there is no case law concerning the right to data portability. The jurisprudence on the right to access (see the commentary on Article 15) may however be of relevance in light of the relationship between the two rights.

It is also worth noting that data portability may be a remedy mandated under EU competition law (Article 102 TFEU) in cases where the failure to provide access to the data might be deemed ‘abusive’ (as it would have an exclusionary effect on equally efficient competitors) if undertaken by a company with a position of market dominance.

C. Analysis

The right to data portability is the latest addition to the rights of the data subject and is intended to empower data subjects. Concerns have however been expressed regarding its broad scope of application, particularly when compared to the data portability remedy available pursuant to competition law. The right is however qualified in important ways. Four criteria might be said to define the limits of the GDPR right to data portability: (i) ‘personal data’; (ii) ‘provided by’ the data subject; (iii) processed pursuant to consent or contract; and, (iv) processed by automated means.

1. The limits of the right to data portability

Unlike, for instance, competition law portability remedies, the right to data portability only applies to ‘personal data’ (see the commentary on Article 4(1)). According to the

---

21 UK Enterprise and Regulatory Reform Act 2013.
22 BIS 2012, p. 5.
23 Consider for example that Microsoft was ordered to provide interoperability information for its software to providers of alternative software products to enable them to interact with servers equipped with Microsoft software in EC Microsoft Decision, at para. 782. This finding was upheld by the General Court in Case T-201/04, Microsoft Corp.
WP29, the right covers pseudonymous data provided that it can be clearly linked to the data subject. Indeed, it follows from Article 11(2) GDPR that the right to data portability shall not apply if the controller is able to demonstrate that it is not in a position to identify the data subject unless the data subject then provides more information that enables the data controller to identify him/her. The controller therefore appears to have no autonomous obligation to acquire additional information for the identification of the data subject.25

The personal data must also be ‘provided by’ the data subject. The WP29 suggests that a distinction should be made between observed data and data actively and knowingly provided by the data subject, which would be included within the scope of the right, and, inferred and derived data, which would be excluded from the scope of the right.26 According to this suggestion, data collected by a device such as a ‘quantified self’ application that tracks an individual’s movements (exercise, sleep etc.) would be within the scope of the right while any insights gleaned on the basis of that information (for example, about the individual’s health status or working patterns) would be excluded from the scope of the right. Such a distinction would ostensibly respect the intellectual property of data controllers (for instance, their application of data analytics to the data ‘provided by’ the data subject) although some practitioners suggest that the actual data provided to individuals may be where intellectual property lies. This is because it may provide an insight into the data gathering process and the types of data collected by the data controller.27

Intellectual property aside, others – such as the European Commission and the Centre for Information Policy and Leadership (CIPL) – have suggested a narrower definition of ‘provided by’. The European Commission’s position is that the WP29 guidelines ‘might go beyond what was agreed by the co-legislators in the legislative process’.28 CIPL distinguishes between the wording of Articles 13 and 20 GDPR: Article 13 refers to information to be provided where personal data are ‘collected from’ the data subject, which, it is implied, is broader than data ‘provided by’ the data subject. CIPL therefore suggests that pursuant to Article 20 ‘there must be a voluntary, affirmative element of ‘providing’ data to the controller, as opposed to collecting data from an individual who may be passive’.29 They distinguish between varieties of ‘observed data’ suggesting that data relating to a wearable device where the individuals ‘willingly and knowingly provide tracking data and sensed data because it is part of the desired service to the individual and conveys a desired benefit to the individual’ should fall within the scope. However, other observed data should not, including network traffic data, as such data ‘falls under the category of technical analysis as it is data generated by systems and not provided by the individual in return for a specific benefit or as part of the service he or she intended to receive’.30 This vision seems to conflict with that of the WP29 which suggests that the

---

27 Boardman and Mole 2017.
30 Ibid.
personal data provided to individuals exercising their right to data portability should include ‘as many metadata with the data as possible at the best possible level of granularity’ as this ‘preserves the precise meaning of exchanged information’.  

Whatever the interpretation of ‘provided by’ adopted however, it is noteworthy that important personal data, such as the online ‘reputation’ that an individual develops as a seller or host in digital marketplaces based on customer reviews, are likely to be excluded from the scope of the right to data portability.

The right also only applies where the individual has either consented to the personal data processing or where the information is processed pursuant to a contract. In instances where personal data processing is reliant on another legal basis (e.g. public interest) the WP29 suggests that it would be good practice nevertheless to develop data portability processes by ‘following the principles governed by the right to data portability’. It gives the example of government services ensuring that past personal income tax filings could be downloaded. Any such processes would however be developed on a voluntary basis. Indeed, Article 17(3) GDPR provides that the GDPR right ‘shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.’

The right applies to processing carried out by automated means. It was noted, with concern, in Council that ‘processing carried out by an automated processing system’ (the wording of an earlier draft) could cover almost anything; however attempts to limit the right to providers of ‘information society services’ or internet services were rejected. It has been suggested that to be automated ‘the means used by the data controller will have to exclude any human intervention during the whole processing’. However, given that the rights of the data subject are generally interpreted expansively, such a restriction seems unlikely.

It is useful to recall that when the right to data portability does not apply to particular personal data (for instance, a user profile) other rights, such as the right of access, the right to object or the right to delete, may remain applicable provided the data concerned are personal data.

2. The responsibilities of the data controller

According to Article 20(1) GDPR the data should be provided to the data subject in a ‘structured, commonly used and machine-readable format’ and the data subject should have the right to transmit those data to another data controller without hindrance. Moreover, Article 20(2) stipulates that, where technically feasible, the data should be transferred directly from one data controller to another.

---

32 Art. 20(3) and rec. 68.
33 WP29 2017, p. 7.
34 Council Interinstitutional File Portability, p 4.
35 Scudiero 2017, p. 6.
The GDPR is silent as to the format of the data transmitted save to stipulate that it should be ‘machine-readable’. Recital 68 does however specify that the data should be available in an ‘interoperable format’, which data controllers ‘should be encouraged to develop’ and, that data portability ‘should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible’. The WP29 defines interoperability as the ‘capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units’. It also notes that ‘structured, commonly used and machine readable’ are specifications for the means, whereas interoperability is the desired outcome. Yet, whether interoperability is desirable is contestable. For instance, it is legitimate to query whose privacy and data use policy will prevail in such circumstances. It is for this reason that some privacy scholars fear a ‘privacy race to the bottom’ if data portability is mandated. Moreover, sceptics suggest that without standards leading to interoperability, the right to data portability may ‘remain more a declaration of principle than a real and effective tool for individual self-determination in the digital environment’. The Commission has published a Communication on ‘ICT Standardization Priorities for the Digital Single Market’, which may be used as a basis on which to develop standards for the purposes of data portability.

The responsibilities of the data controller are therefore difficult to grasp. As ‘technically feasible’ is not defined by the GDPR, some data controllers may claim that direct controller-to-controller data transfers are not possible. Scudiero suggests that a new export-import model will be needed, and that controllers will need to ‘plan specific investments in order to adapt their IT systems to this new legal perspective’. For its part, the WP29 recommends that data controllers offer several options to the data subject. They suggest, for instance, that data subjects should be offered an opportunity to directly download the data as well as to transmit it directly to another data controller, and that this could be implemented by making an Application Programme Interface (API) available. Cormack expresses doubt regarding the viability of this solution, noting that many organizations will hold their data on internal databases, that are securely firewalled from internet access, as opposed to APIs. He also warns that as the majority of data subjects are unlikely to ever use their own account on this API, it ‘will create a large number of idle accounts, likely to have simple or default passwords’ while good security practice has been to remove such accounts.

A further query for data controllers concerns the data of third-party data subjects. The WP29 guidelines suggest that the recipient data controller is responsible for ensuring that portable data provided are relevant and not excessive with regard to the new data processing. This obligation is however contestable. As CIPL notes, it is not clear that

37 Ibid., p.13.
38 Grimmelmann 2009, p.1194.
40 Ibid., p.3.
41 WP29 2017, p.5.
42 Cormack 2017.
there is an obligation to receive this data on the recipient controller; ‘it may be impractical or disproportionate to require the receiving controller to assess the data it receives; unrealistic to require the receiving controller to provide individuals with a full notice about data use before the request for transmission’.43

Article 20(4) GDPR explicitly states that the right to data portability should not adversely affect the rights and freedoms of others. Scudiero notes that this seems to imply that the right enjoys a lower rank compared to the rights and freedoms of others.44 However, the WP29 states that, for example, ‘a potential business risk cannot, in and of itself serve as a basis for a refusal to answer a portability request’.45

3. The challenges of data portability

Data security will be a major challenge for data controllers. The opportunities for data breach are numerous: an individual may attempt to exercise the right fraudulently (which would also constitute a data security breach); the data may be interfered with during transmission between controllers; or, the data may be accessed once on the data subject’s personal devices. For instance, where controllers have had no significant prior contact with the data subject, or where they hold only indirect identifiers for him or her, authentication of identity may be difficult. Articles 11(2) and 12(6) GDPR might be of use in such circumstances as they respectively allow the data subject to provide more information to the data controller to enable his or her identification and enable controllers with reasonable doubts regarding the identity of a data subject to request further information to confirm identity.

These data security risks should be taken into consideration by the data controller when conducting its data protection impact assessment. For its part, the WP29 simply recognizes that data portability ‘may also raise some security issues’ while highlighting that the data controller will remain responsible for ‘taking all the security measures needed to ensure that personal data is securely transmitted’.46 Commentators have offered various solutions to alleviate these concerns: for instance, Scudiero suggests that Article 20 ‘should have been drafted so as to provide a clear reference to a minimum standard of security measures’47 while CIPL recommends that ‘solutions are found allowing individuals to suspend or freeze the portability mechanisms with respect to their accounts if there is suspicion that the account has been compromised, and a delay feature to enable robust verification of identity’.48

43 CIPL 2017, p.5.
44 Scudiero 2017, p.9.
45 WP29 2017, p.10.
46 Ibid., p.15.
47 Scudiero 2017, p.7.
48 CIPL 2017, p. 11.
Select bibliography

Legislation


HIPAA: Health Insurance Portability and Accountability Act, Public Law 104-191 (104th Congress).

Philippine Data Privacy Act 2012: Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes, Republic Act No. 10173 (‘the Data Privacy Act of 2012’).

UK Enterprise and Regulatory Reform Act 2013: Enterprise and Regulatory Reform Act, Chapter 24 (c. 24).


Academic writings


Papers of data protection authorities


Reports


Others

Article 24

Responsibility of the controller

Christopher Docksey

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Relevant recitals

(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk
should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

(77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

CLOSELY RELATED PROVISIONS

Article 5 (Principles relating to processing of personal data) (see too recital 39); Article 25 (Data protection by design and by default) (see too recital 78); Article 30 (Records of processing activities) (see too recital 82); Article 32 (Security of processing) (see too recital 83); Article 35 (Data protection impact assessment) (see too recitals 84 and 89-93); Articles 37-39 (Data protection officer) (see too recital 97); Articles 40-41 (Codes of conduct) (see too recitals 98-99); Articles 42-43 (Certification) (see too recital 100); Article 47 (Binding corporate rules) (see also recitals 108 and 110); Article 83 (General conditions for imposing administrative fines) (see too recitals 148 and 150-151).

RELATED ARTICLES IN LED [Directive (EU) 2016/680]

Articles 19 (Obligations of the controller) (see too recitals 50 to 52); Article 20 (data protection by design and by default) (see too recital 53); Article 24 (Records of processing activities) (see too recital 56); Article 25 (Logging) (see too recital 57); Article 27 (data protection impact assessment) (see too recital 58); Article 29 (security of processing) (see too recital 60); Articles 32-34 (Data protection officer) (see too recital 63).

RELATED ARTICLES IN EPD [Directive 2002/58/EC, as amended]

Article 4(1) and (1a) (security of processing and implementation of a security policy) (see too recital 20).

RELEVANT CASE LAW

CJEU

Case C-553/07, College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer, judgment of 7 May 2009 (ECLI:EU:C:2009:293).
Case C-362/14, Schrems v Data Protection Commissioner, judgment of 6 October 2015 (ECLI:EU:C:2015:650).
A. **Rationale and Policy Underpinnings**

Article 24 is entitled 'Responsibility of the controller,' but can be viewed as imposing accountability obligations. The principle of accountability is one of the central pillars of the GDPR and one of its most significant innovations. It places responsibility firmly on the controller to take proactive action to ensure compliance and to be ready to demonstrate that compliance.

The term ‘accountability’ is not new for data protection law. In its original sense of responsibility for specific tasks and duties it was present in the original OECD Guidelines and was implicit in the data quality requirements of Convention 108 and in Article 6(2) of the DPD.

However, the new meaning of the accountability principle could already be seen in the security requirements in Article 17 of the DPD and in the extra-statutory procedure for BCRs (see discussion below). Accountability in this sense requires that controllers put in place internal policies and mechanisms to ensure compliance and provide evidence to demonstrate compliance to external stakeholders, including supervisory authorities.

The problem that the new accountability principle seeks to resolve was summarised by the Article 29 Working Party (WP29) in 2009 as follows:

[C]ompliance with existing legal obligations often is not properly embedded in the internal practices of organizations. Frequently, privacy is not embedded in information processing technologies and systems. Furthermore, management, including top level managers, generally are not sufficiently aware of and therefore actively responsible for the data processing practices in their own organizations…. Unless data protection becomes part of the shared values and practices of an organization, and unless responsibilities for it are expressly assigned, effective compliance will be at risk and data protection mishaps will continue. … The principles and obligations of [data protection law] should permeate the cultural fabric of organizations, at all levels, rather than being thought of as a series of legal requirements to be ticked off by the legal department.’¹

To address this situation, the WP29 proposed that the Commission consider accountability-based mechanisms, with particular emphasis on the possibility to include a principle of ‘accountability’ in the legislative reform. This principle would strengthen the role of the data controller and increase its responsibility.²

The following year, the WP29 developed its analysis in detail in its Opinion on Accountability. It warned that the then legal framework had not been fully successful in ensuring that data protection requirements translate into effective mechanisms that deliver real protection, and proposed a draft accountability clause for new legislation:

**Article X - Implementation of data protection principles**

¹ WP29 2009, p. 19.
² WP29 2010, p. 3.
1. The controller shall implement appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with.

2. The controller shall demonstrate compliance with paragraph 1 to the supervisory authority on its request.  

B. Legal Antecedents

1. EU legislation

The precursor to the principle of accountability is the principle of responsibility, which can be found in Article 6(2) DPD: ‘It shall be for the controller to ensure that paragraph 1 is complied with.’ In addition, Article 17(1) DPD required data controllers to implement measures of both a technical and organisational nature to ensure security of processing.

Article 4 EPD imposes an obligation to take appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented.

2. International treaties

The 1980 OECD Privacy Guidelines included an Accountability Principle similar to the principle of responsibility in Article 6(2) DPD. Article 14 of the Guidelines states: ‘A data controller should be accountable for complying with measures which give effect to the principles stated above.’ The updated OECD Privacy Guidelines from 2013 maintain the original Accountability Principle but add the new meaning of accountability, in the sense of proactive and demonstrable compliance, in a new Part Three on Implementing Accountability. This sets out the key elements of what it means to be an accountable organisation, including basic elements such as those set forth in Article 24 GDPR and common elements of the principle (discussed below).

The OECD approach forms the basis of the Asia-Pacific Economic Cooperation (APEC) Privacy Framework of 2005, which includes a similarly worded accountability principle as the final principle in a list of nine Information Privacy Principles. An accountability mechanism, certified by an APEC-recognised independent third party known as an Accountability Agent, also features in the APEC Cross Border Privacy Rules (CBPR). The CBPR System consists of four elements: (1) self-assessment of data privacy policies and practices against the requirements of the APEC Privacy Framework; (2) compliance review; (3) recognition/acceptance; and (4) dispute resolution and enforcement. In 2014, the WP29 together with the APEC group issued jointly a ‘Referential’ that maps the differences and similarities between BCRs in the EU and the Cross-Border Privacy Rules (CBPR) system among the APEC countries.

---

3 Ibid., p. 10.
4 See also Art. 16 of the Guidelines, with regard to transborder flows of personal data: ‘A data controller remains accountable for personal data under its control without regard to the location of the data’.
5 The APEC group is an intergovernmental forum comprised of the 21 Pacific Rim member economies, focused primarily upon trade and economic issues.
6 See Cross Border Privacy Rules System.
7 WP29 2014A.
The ‘Accountability principle’ was explicitly included in point 11 of the ‘Madrid Resolution’, a Joint Proposal on International Standards for the Protection of Privacy adopted by the International Conference of Data Protection and Privacy Commissioners on 6 November 2009:

The responsible person shall:

a. Take all the necessary measures to observe the principles and obligations set out in this Document and in the applicable national legislation, and

b. have the necessary internal mechanisms in place for demonstrating such observance both to data subjects and to the supervisory authorities in the exercise of their powers, as established in section 23.

An accountability approach is also present in recent ISO International Standards. Standard 29190 sets out a Privacy Capability Assessment Model which provides high-level guidance about how to assess the level of an organisation’s ability (capability) to manage privacy-related processes and these processes’ efficiency and effectiveness. Standard 27018 on cloud computing has been described as ‘an instrument that assists the PII processor to comply with the principle of accountability requirements.’

Finally, in parallel to Article 24 GDPR, the ongoing modernisation process for the modernisation of Convention 108 provides for a modern accountability obligation in Article 8bis on ‘additional obligations’:

Each Party shall provide that controllers and, where applicable, processors take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate, in particular to the competent supervisory authority provided for in Article 12bis, that the data processing under their control is in compliance with the provisions of this Convention.

3. National legislation

National legislation and interpretation by supervisory authorities have played a significant role in developing accountability, both in Europe and worldwide. Examples include, first and foremost, Canada, where the principle of accountability is set forth in Schedule 1 of the Personal Information Protection and Electronic Documents Act (PIPEDA) of 2000. PIPEDA requires organizations to comply with a set of legal obligations that are based on ten Fair Information Principles, of which accountability is the first. In 2012 the guidance document, ‘Getting Accountability Right with a Privacy Management Program,’ explained that accountability ‘is the first among the principles because it is the means by which organizations are expected to give life to the rest of the fair information principles that are designed to appropriately handle and protect the personal information of individuals.’

---

9 De Hert and others 2014, p. 19.
10 Art. 8bis Convention 108 (modernised).
11 Canadian Privacy Commissioners 2012, p 3.
The first principle requires policies and procedures that promote good practices which, taken as a whole, constitute a privacy management program. This would include implementing procedures for protecting personal information, establishing procedures for receiving and responding to complaints and inquiries, training staff on policies, and developing information to explain those policies.

The Canadian approach requiring a Privacy Management Programme can also be found in the Best Practice Guide issued by the Hong Kong Privacy Commissioner for Personal Data and in the Colombian regulator’s Guide for the Implementation of the Principle of Accountability, which specifically refers to the Canadian guidance document.

In 2015, the CNIL in France produced a standard defining what is required in practice to be accountable, inspired in part by the then Proposal for the GDPR. The Standard has 25 requirements, which must all be respected, divided into three areas: internal organisation, methodology for achieving compliance, and the handling of claims and incidents. Controllers that comply with the new standard are able to obtain an ‘accountability seal’ from the CNIL (‘Label Gouvernance Informatique et Libertés’).

Also, in 2015, the Australian Information Commissioner published guidelines on the Australian Privacy Principles (APPs) laid down in schedule 1 of the federal Privacy Act of 1988. The first APP covers the open and transparent management of personal information including having a privacy policy. The 2015 guidance, known as the Privacy Management Framework, sets out four steps to ensure compliance: embedding a culture of privacy, establishing robust and effective privacy policies, evaluating their effectiveness, and enhancing the response to privacy issues.

Finally, the US Federal Trade Commission (FTC) has authority under Section 5 of the Federal Trade Commission Act to take enforcement action which may require US companies to take steps to remedy unlawful behaviour. Its enforcement actions may require firms to adopt comprehensive privacy programs as part of a binding consent decree.

C. Analysis

The GDPR marks a fundamental shift in approach to data protection. Under Articles 18 and 19 DPD controllers were required to notify their supervisory authority of their data processing operations. Whilst in principle this enabled DPAs to check on the data processing being notified, in practice they did not have the resources to examine all this data. It also had the danger that controllers may have felt that the notification process had discharged their responsibilities.

The GDPR has removed the obligation of notification to DPAs. Instead, the principle of

---

12 Privacy Management Programme 2014.
14 CNIL 2014.
15 Australian Privacy Management Framework.
16 FTC Privacy & Security, see for example FTC Snapchat file.
accountability enshrined in Article 24 GDPR has shifted the emphasis to the controller, requiring it to take action itself, subject to the possibility to be asked at any time to demonstrate compliance. Processors are covered by specific accountability-related provisions such as Article 30 (records) and Article 32 (security), but Article 24 places responsibility solely on the controller to comply with the obligations under the GDPR at all stages of processing, from beginning to end.

1. Terminology

Accountability is a common term in English, with implications of responsibility, answerability and good governance. The understanding of the term is regarded as a core issue of political science because of the danger that organisations may often attempt to be ‘accountable’ in multiple and conflicting senses, leading to what Koppel describes as ‘multiple accountabilities disorder’. In response he has developed a typology of five accountability concepts: transparency (an accountable organisation must explain or account for its actions), liability (individuals and organisations should be held liable for their actions), controllability (did the organisation do what its principal desired?), responsibility (fidelity to the rules), and responsiveness (an organisation’s attention to direct expressions of the needs and desires of its constituents or clients).17

Under this typology the term accountability was originally used in data protection law in the sense of responsibility, a controller being responsible for ensuring compliance with the data protection rules, particularly those on data quality.18 This meaning can be seen in the original Accountability Principle at paragraph 14 of the OECD Guidelines in 1980 and in Article 5(2) GDPR. However, its meaning has developed to the new and more demanding concept of proactive and demonstrable compliance set forth in Article 24 of the GDPR, as well as in the 2013 revision of the OECD Guidelines and the draft modernised Convention 108. Under the above typology the new GDPR version of accountability may be seen as responsiveness, transparency and, as discussed below, liability.

In the GDPR the word ‘accountability’ has been translated literally as ‘accountability’ in some languages, e.g. ‘Rechenschaftspflicht’ in German, and as ‘responsibility’ in others, e.g. ‘responsabilité’ in French. In Polish it is has overtones of financial accountability (‘rozliczalność’). Perhaps the most useful translations are in Spanish, which use the concept of ‘proactive responsibility’ (‘responsabilidad proactiva’) in Spain and ‘demonstrable responsibility’ (‘responsabilidad demostrada’) in Colombia. These translations reflect two of the key elements of accountability discussed below, of actively developing compliance and being able to demonstrate compliance. It is best to regard the principle set forth in Article 24 of the GDPR as a term of art with its own specific meaning. This has been described as ‘organisational responsibility … as a means to assure data protection and for firms to satisfy domestic legal obligations’.19 It could also be summarised as ‘proactive and demonstrable organisational responsibility’. To understand the principle of accountability better it is helpful to examine its core statutory elements and its commonly accepted elements in practice.

18 Case C-553/07, Rijkeboer, at para. 48.
19 Privacy Bridges 2015, Bridge 8.
2. The statutory elements of accountability under the GDPR

First, accountability requires controllers and processors to take responsibility for the personal data they handle. In this sense it was present in Article 6(2) DPD and has been carried over into Article 5(2) GDPR.

Second, Article 24 GDPR requires controllers and processors to assess and to put in place appropriate and effective measures to ensure compliance with the principles and obligations set out in the GDPR. These have been described as ‘compliance programs’ by the WP29.20

The final sentence of Article 24(1) notes that ‘those measures shall be reviewed and updated where necessary.’ The Commission Proposal originally added that, ‘if proportionate, this verification shall be carried out by independent internal or external auditors.’ The element of audit by the controller remains in Article 28(3)(h), as part of the obligation on the processor to demonstrate compliance, in Article 39(b), as part of the tasks of the DPO, and in Article 47, as part of the mechanisms under a BCR to ensure verification of compliance. The Parliament also proposed to add that ‘compliance policies should be reviewed at least every two years and updated where necessary.’ Whilst this specific period was not adopted, as a matter of good practice there should be provision for review at regular intervals and for updating policies following the results of such a review or a relevant change in circumstances.21 This latter could be brought about by a change in the organisation of the controller, a processor or data recipients, or a development in the law or legal interpretation affecting the processing by the controller.22

The word ‘appropriate’ means that accountability is scalable, enabling the determination of the concrete measures to be applied depending on the processing being carried out, the types of data processed and the level of risk to data subjects of that processing. Thus, the second paragraph of Article 24 requires that, ‘(w)here proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.’

Third, Article 24 GDPR requires controllers and processors to be able to demonstrate that they have the appropriate systems in place to ensure compliance, whether to supervisory authorities assessing compliance, to customers or to the public at large. This obligation may also be found in Article 5(2) GDPR, which refers specifically to ‘accountability’.

The GDPR does not define what is necessary to demonstrate compliance, but Article 24(3) notes that adherence to approved codes of conduct under Article 40 or approved certification mechanisms, as well as data protection seals and marks, under Article 42(1) ‘may be used as an element by which to demonstrate compliance.’ In 2010 the WP29 argued that its recommended provision on accountability could foster the development of certification programs or seals: ‘Such programs would contribute to prove that a data controller has fulfilled the provision; hence, that it has defined and implemented appropriate measures which have been periodically

---

20 WP29 2010, p. 4.
21 See, by analogy, the CJEU reasoning on reassessment of adequacy following a change of circumstances in Case C-362/14, Schrems, at para 146.
22 Canadian Privacy Commissioners 2012, pp. 16-18.
Article 32(3) also refers to these mechanisms, as an element to demonstrate compliance with the obligation of security of processing. Similarly, Article 25(3) provides that an approved certification mechanism under Article 42 may be used as an element to demonstrate compliance with the requirements data protection by design and default.\textsuperscript{24}

Finally, in addition to these two mechanisms, recital 77 notes that guidance on the demonstration of compliance could also be provided by means of ‘guidelines provided by the Board or indications provided by a data protection officer.’

In practice, what is required to demonstrate compliance to supervisory authorities will depend on the processing in question. In its Opinion on the principle of accountability, the WP29 gave two examples:

[I]n simple and basic cases, such as for the processing of personal data related to human resources for the establishment of a corporate directory, the “obligation to demonstrate” … could be fulfilled easily (through for instance the information notices that were used; the description of basic security measures etc.). On the contrary, in other more complex cases, such as for instance the use of innovative biometric devices, fulfilling the “obligation to demonstrate” could need further requirements. The controller may have for instance to demonstrate that it undertook a privacy impact assessment, that the staff involved in the processing are trained and informed regularly, etc.\textsuperscript{25}

The WP29 also recalled that:

Transparency is an integral element of many accountability measures. Transparency vis-à-vis the data subjects and the public in general contributes to the accountability of data controllers. For example, a greater level of accountability is achieved by publishing privacy policies on the Internet, by providing transparency in regard to internal complaints procedures, and through the publication in annual reports.\textsuperscript{26}

3. The common elements of accountability in practice

In 2009, the Global Accountability Dialogue, also known as the \textit{Galway Project}, brought together experts from a wide range of sectors – industry, civil society, academia, government, data protection commissioners and privacy regulators. They identified, for the first time, five ‘common elements’ of accountability.\textsuperscript{27} Later that year, an accountability principle was included

\textsuperscript{23} WP29 2010, p. 17.
\textsuperscript{24} It should be noted that Art. 42(4) provides that a certification does not reduce the responsibility for compliance of the controller or the processor.
\textsuperscript{25} WP29 2010, p. 13.
\textsuperscript{26} Ibid., p. 14.
\textsuperscript{27} Galway Project 2009, led by the Irish Data Protection Commissioner and the Centre for Information Policy Leadership. The five elements were:
1. Organisation commitment to accountability and adoption of internal policies consistent with external criteria.
2. Mechanisms to put privacy policies into effect, including tools, training and education.
in the ‘Madrid Resolution’ and the WP29 made initial comments on accountability in its Future of Privacy Opinion. This opinion was followed by a detailed list of elements in the WP29 Opinion on the principle of accountability. In 2015 the Privacy Bridges Report presented to the 37th Annual International Privacy Conference in Amsterdam considered elements that could be implemented in both the EU and the United States. The draft Explanatory Report on the modernisation of Convention 108 also explains the elements of the principle of accountability. Finally the Explanatory Memorandum to the GDPR sets out elements of accountability in addition to the core, statutory elements of accountability in the GDPR itself.

The common elements in these various documents may be summarised as follows:

1. Appointment of data protection professionals to assure internal implementation: the GDPR requires DPOs to have expert knowledge, to report to top management, and for there to be provision for their professional development and necessary resources.
2. Organisational commitment to accountability and the approval and oversight of internal policies by top management.
3. Mapping of processing activities, assessment of purpose specification, and assessment of the risks to individuals ‘by virtue of their nature, their scope or their purpose’. The WP29 has also referred to ‘economic and reputational risks’. The risk assessment may lead to conducting a DPIA.
4. Adoption of internal policies and processes to implement relevant data protection requirements for the particular processing operations carried out by the controller, which are binding on all corporate units and staff members in the organisation.
5. Assignment of responsibility for data protection to designated persons at different levels in the organisation with responsibility for compliance.
6. Mechanisms to put internal policies and processes into effect and make them effective in practice. These may include tools, staff training and awareness, and instructions about the collection and processing of data. In particular there should be internal policies to implement the principles of data protection by design and data protection by default.
7. Systems for internal ongoing oversight, review and updating and external verification.

---

29 WP29 2010, pp. 11-12.
30 Privacy Bridges 2015, Bridge 8.
32 Rec. 97 GDPR.
33 Art. 38(3) GDPR.
34 Art. 38(2) GDPR.
35 EDPS 2016, p. 2.
36 WP29 2013.
37 Rec. 74 GDPR.
38 See WP29 2010, p. 3.
39 WP29 2017A, pp. 8-12.
40 Canadian Privacy Commissioners 2012, p. 10.
41 Rec. 78 GDPR.
42 Art. 24(1), final sentence, GDPR.
internal compliance reports, external audits, third-party certification and/or seals to monitor and assess whether the internal measures are effective.\textsuperscript{43}

8. Transparency of these adopted measures for data subjects, regulators and the general public.\textsuperscript{44}

9. Means for remediation and external enforcement, including response mechanisms that provide means for individuals to complain about privacy violations\textsuperscript{45}, means for data breach notification\textsuperscript{46} and means for organisations to address any discovered deficiencies, and redress for violations of the privacy requirements.

4. Scalability – Nature of Processing and Level and Likelihood of Risk

Controllers must tailor the measures to the concrete specifics of the data controller and the data processing operations in question. The technical and organisational measures required under the principle of accountability must be ‘appropriate’ in view of the two factors specified in Article 24, namely the nature of the processing and the likelihood and severity of risk. The GDPR introduces the criterion of likelihood of risk in addition to that of the level or severity of risk in Article 17 DPD. Recital 74 explains that the ‘likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing.’

The WP29 has stressed that:

\begin{quote}
[T]he rights of individuals … must be just as strong even if the processing in question is relatively ‘low risk’. Rather, the scalability of legal obligations based on risk addresses compliance mechanisms. This means that a data controller whose processing is relatively low risk may not have to do as much to comply with its legal obligations as a data controller whose processing is high-risk.\textsuperscript{47}
\end{quote}

Normally the size of the organisation concerned does not per se determine the level of compliance required. One provision of the GDPR, Article 30, provides that organisations employing fewer than 250 persons do not have to respect the obligation to keep records of processing activities. This is subject to two caveats. First, the obligation applies if the processing they carry out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes sensitive data. Second, controllers remain subject to the general obligation in Article 24 to be able to demonstrate compliance.

Recital 75 GDPR explains that risks ‘may result from personal data processing which could lead to physical, material or non-material damage’. It contains an extensive but not exhaustive list of examples of processing which may give rise to such risks and thus should be borne in mind. Examples given by the legislator include processing which may give rise to discrimination, identity theft or fraud, the processing of sensitive data, and the processing of a large amount of

\textsuperscript{43} Rec. 100 GDPR.
\textsuperscript{44} Raab 2017, p. 344.
\textsuperscript{45} Art. 38(4) GDPR.
\textsuperscript{46} Rec. 85 and 86 GDPR.
\textsuperscript{47} WP29 2014B, p. 2.
personal data which affects a large number of data subjects.

The WP29 has pointed out that some measures are ‘staples’ that will have to be implemented in most data processing operations. These would include drafting internal policies and procedures implementing those policies, e.g. procedures to handle access requests and complaints.48 Where the organisation is larger and more complex, and/or where there is a higher level of risk, the GDPR requires controllers to do more, and sets out a number of specific accountability-related tools to this effect.

5. Accountability-related measures

The GDPR accompanies the principle of accountability with a suite of tools for controllers, described by the WP29 as ‘accountability based mechanisms … as a way of encouraging data controllers to implement practical tools for effective data protection.’49

Article 22(2) of the Commission Proposal listed five measures ‘in particular’: documentation, security, data protection impact assessments, prior authorisation or consultation and the DPO. These examples are not retained in the text finally adopted. Instead Article 24(3) of the GDPR specifically mentions two different mechanisms, codes of conduct and certification, which may be used as an element by which to demonstrate compliance with the obligations of the controller.

In addition, the GDPR underlines the importance for accountability of a number of other mechanisms: the principles of data protection by design and default under Article 2550, the keeping of records under Article 30, data protection impact assessments (DPIAs) under Article 3551, the Data Protection Officer (DPO) under Articles 37-3952, and Binding Corporate Rules (BCRs) under Article 47.53

Many of these accountability-based mechanisms are good practice for controllers, which the GDPR has rendered legally binding in some cases. The Commission Proposal,54 the WP29 and national DPAs have strongly underlined the complementary nature of these tools, which all promote accountability and good governance.

In its 2010 Opinion, the WP29 distinguished between the minimum requirements of a future accountability obligation, a ‘first tier’ binding on all controllers, and a ‘second tier’ of accountability architecture, whereby controllers that wish to do so achieve a higher level of accountability.

---

49 Ibid., p. 3.
50 See rec. 78 GDPR and see the discussion of Art. 25.
51 The WP29 regards DPIAs as ‘important tools for accountability’ as they can help controllers both to comply with the GDPR and to demonstrate compliance with it, see WP29 2017A.
52 The WP29 regards the DPO as a ‘cornerstone of accountability’ in the sense that the DPO can facilitate compliance through the implementation of other accountability tools such as DPIAs and audits and can act as an intermediary between internal and external stakeholders, see WP29 2017B, p.4. See also EDPS 2012, p. 3, where the EDPS stressed the role of DPOs in accountability.
53 The WP29 has identified binding corporate rules as ‘a way to implement data protection principles on the basis of the accountability principle’, see WP29 2010, p. 15.
54 EC Communication 2010, pp. 6-7.
compliance through voluntary use of tools such as DPIAs and DPOs. In the meantime, although minimum standards are now enshrined in the GDPR, the WP29 in its various Opinions and Guidelines has consistently urged controllers as a matter of good practice to use accountability mechanisms to the full and not to limit their use to the minimum required by statute (see discussion below), the aim being to aim for a high standard of effective compliance.

6. Accountability and the law

Two quite different questions arise. First, does the principle of accountability itself impose new obligations on data controllers and processors? Secondly, if a controller respects the principle of accountability and implements all the necessary measures, does this provide a ‘safe harbour’ in the event of an unexpected violation, such as a data breach?

Turning to the first-listed question, the responsibility of the controller under Article 5(2) to ensure compliance with the principles relating to processing of personal data in Article 5(1) already existed under under Article 6(2) DPA. However, the proactive obligation to adopt appropriate measures and the obligation to be able to demonstrate compliance are new obligations which, quite apart from any failure to respect applicable accountability-related obligations, would in themselves render controllers liable for non-compliance.

In this respect, the wording of Article 24 is significant. The references to ‘risks of varying likelihood and severity for the rights and freedoms of natural persons’ are echoed both in accountability-related obligations55 and in the provisions on administrative fines in Article 83. This requires due regard to be paid in the first instance to the nature, gravity and duration of the infringement and to any other applicable aggravating or mitigating factors. Article 24(3) itself refers to two mitigating factors that may be taken into account, the use of codes of practice and certification.

This link between accountability and sanctions was specifically made by the WP29 in 2010:

> The proposed system can only work if data protection authorities are endowed with meaningful powers of sanction. In particular, when and if data controllers fail to fulfil the accountability principle, there is a need for meaningful sanctions. For example, it should be punishable if a data controller does not honour the representations it made in binding internal policies. Obviously, this is in addition to the actual infringement of substantive data protection principles.56

Turning to the second-listed question, the response is, first, that an accountable controller will have put in place robust programmes that are more likely to be in compliance and less likely to be in breach of the law. Second, the presence of such programmes, documented as necessary, would certainly be an element taken into account should a problem arise. Article 83(2)(b)(c) and (d) lay down the general conditions for imposing administrative fines, and requires due regard to

55 Regarding privacy by design, see Art. 25(1). Regarding security, see Art. 32. Regarding DPIAs, see rec. 84 and 90.
56 WP29 2010, p. 17.
be taken of the circumstances when deciding on whether to impose a fine and on the amount of the administrative fine, and, in particular for present purposes:

‘(b) the intentional or negligent character of the infringement;
(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
(d) 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’ (that is, respect for the requirements of data protection by design and by default and of security of processing).

With regard to individual cases brought by data subjects, the accountability obligation on controllers to be able to demonstrate compliance may well affect the burden of proof. Whilst the legal burden of proof is still borne by the data subject, it is argued that ‘the evidential burden of proof should de facto shift to the controller as soon as the data subject has offered prima facie evidence of an unlawful processing activity.’

This strong relation between accountability and key obligations and sanctions in the GDPR is a powerful incentive for encouraging proactive compliance. A fully accountable controller is unlikely to be in a situation of non-compliance and thus unlikely to be sanctioned in the event of unexpected events.

7. Conclusion: the development of accountability

The concept of accountability lies at the root of the new approach to compliance demanded by the GDPR. It is crucial for controllers to take active responsibility for ensuring compliance and develop an accountability culture at all levels of their organisation.

For some controllers the link to sanctions for non-compliance will provide the necessary motivation. For others respect for privacy and data protection will become part of their ethical framework, and ethical standards will drive the use of the accountability-related tools discussed above, in particular DPIAs and data protection by design and data protection by default.

Finally, accountability is increasingly an international concept, and will be key to both facilitating and enhancing compliance by controllers using the new technologies of big data, cloud computing, and artificial intelligence, both in the EU and abroad.

57 Van Alsenoy 2016, p. 9.
58 EDPS 2015. See also Abrams 2015.
59 The Information Accountability Foundation has updated the five essential elements of the Galway Project to respond to the challenges of big data and most recently artificial intelligence, see AI Essential Elements in IAF 2017, p. 11. See also Raab 2017 and materials referred to therein.
Select Bibliography

Legislation


Madrid Resolution: 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).

Academic writings


Papers of data protection authorities


WP29 2017A: 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).


Reports


Docksey
**Article 25**

**Data protection by design and by default**

*Prof. Lee Bygrave*

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

**Relevant recital**

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.
CLOSELY RELATED PROVISIONS

Article 5(2) (accountability) (see too recital 11); Article 6(4)(e) (compatibility); Article 22 (automated individual decision-making, including profiling) (see too recital 71); Article 24 (responsibility of controllers); Article 28 (processors) (see too recital 81); Article 32 (security of processing) (see too recital 83); Article 34(3)(a) (communication of personal data breach to data subject) (see too recitals 87 and 88); Article 35 (data protection impact assessment) (see too recital 84); Article 40 (codes of conduct); Article 83(2)(d) (fines)

RELATED ARTICLES IN LED [Directive (EU) 2016/680]

Article 4(4) (controller responsibility) (see too recital 50); Article 19 (obligations of controller); Article 20 (data protection by design and by default) (see too recital 53); Article 22 (processor) (see too recital 55); Article 24(1)(i) (records of technological and organisational security measures); Article 25 (logging) (see too recital 57); Article 27 (data protection impact assessment) (see too recital 58); Article 29 (security of processing) (see too recital 60); Article 31(3)(a) (communication of personal data breach to data subject)

RELATED ARTICLES IN EPD [Directive 2002/58/EC]

Article 14 (technical features and standardisation) (see too recital 33)

RELEVANT CASE LAW

CJEU

Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd and Seitlinger and Others, judgment of 8 April 2014 (ECLI:EU:C:2014:238).
Case C-131/12, Google Spain v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014 (ECLI:EU:C:2014:317).

ECtHR

I v Finland, Appl. No. 20511/03, Judgment of 17 July 2008.
A. Rationale and Policy Underpinnings

Article 25 is aimed at ensuring that the design and development of systems for processing personal data take due account of core data protection principles such that the latter are effectively integrated into the resulting systems. This entails ensuring that the safeguarding of privacy-related interests receives serious consideration throughout the lifecycle of information systems development – and not just towards the end of the lifecycle. The basic rationale for this endeavour is a belief that building data protection principles into information systems architecture will substantially improve the principles’ traction. Part and parcel of this rationale is recognition of the powerful regulatory potential of information systems architecture, particularly its ability to shape human conduct in ways that are often more effective than the imposition of law laid down by statute or contract.

At the same time, Article 25 exemplifies and elaborates the increased emphasis in the GDPR on making controllers accountable and responsible for their data processing operations. Article 25 is thus closely linked to the provisions of Articles 5(2) and 24.

Article 25 springs out of a policy discourse that commonly goes under the nomenclature ‘Privacy by Design’ (PbD). Closely linked to this discourse is an older policy discourse centred on the creation of ‘Privacy-Enhancing Technologies’ (PETs) – i.e. technological mechanisms that promote respect for privacy-related interests. During the last decade, PbD ideals have become a staple part of data protection authorities’ regulatory approach. In 2010, the 32\textsuperscript{nd} International Conference of Data Protection and Privacy Commissioners unanimously passed a resolution recognising ‘Privacy by Design as an essential component of fundamental privacy protection’ and encouraging ‘the adoption of Privacy by Design’s Foundational Principles … as guidance to establishing privacy as an organisation’s default mode of operation’. WP29 has followed up this resolution in, \textit{inter alia}, policy pronouncements concerning internet technology.

B. Legal Antecedents

1. EU legislation

Article 25 has no exact equivalent in the DPD. The latter contained, however, provisions with a similar thrust as Article 25, albeit with a pronounced security focus. Recital 46 DPD mentioned the need to take ‘appropriate technical and organizational measures’ for protection of data subjects’ rights and freedoms ‘both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing’. The recital went on to stipulate that ‘these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected’. Article 17 DPD was in a similar vein, although the protective measures it listed concerned information security rather than data protection more generally.

---

\footnote{Further on the evolution and parameters of these policy discourses, see e.g. Cavoukian 2009, Schaar 2010, Rubinstein 2012, Klitou 2014, ENISA 2014, Bygrave 2017A.}

\footnote{See e.g. WP29 2014.}
In respect of electronic communications, Article 4(1) EPD replicates the security focus of the DPD by requiring a ‘provider of a publicly available electronic communications service’ to ‘take appropriate technical and organisational measures to safeguard security of its services’. However, recital 30 EPD reaches beyond a security remit by encouraging design measures that give effect to the minimisation principle: ‘Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum’. Article 14(3) EPD also reaches beyond a security remit by requiring the adoption of measures ‘to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data’. This provision parallels Article 3(3)(e) of the Radio Equipment Directive (2014/53/EU) which empowers the Commission to issue delegated legislation requiring that certain classes of radio equipment ‘incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected’.

2. International treaties

The ideals of Article 25 are poorly reflected in Convention 108 as first adopted. However, the 2016 proposal to modernise the Convention introduces a set of provisions in Article 8bis embracing requirements for ‘data protection by design’, but using different formulations than found in Article 25. Article 8bis(2) stipulates that a state party shall require ‘controllers and, where applicable processors’ to ‘examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms’. Article 8bis(3) requires a state party to provide ‘that controllers, and, where applicable, processors, implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing’. Article 8bis(4) permits a state party, ‘having regard to the risks arising for the interests, rights and fundamental freedoms of the data subjects’, to modify its law giving effect to the requirements of the preceding provisions ‘according to the nature and volume of the data, the nature, scope and purpose of the processing and, where appropriate, the size of the controller or processor’.

3. National legislation

Prior to adoption of the GDPR, Germany’s Federal Data Protection Act of 1990 came closest, at the national level, to embracing the thrust of Article 25. Under the nomenclature ‘Datenvermeidung und Datensparsamkeit’ (data avoidance and data economy), section 3a of the Act required information systems to be designed with the aim of processing as little personal data as possible. Elaborating on this requirement, section 3a stipulated that personal data shall be pseudonymised or anonymised insofar as is reasonable in relation to the desired level of protection. A similar stipulation is contained in section 71(1) of Germany’s Federal Act of 30 June 2017 to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680. The provisions of section 71 otherwise reproduce the requirements of Article 25 GDPR, albeit with slight differences in syntax.
4. Case law

The CJEU has yet to rule directly on the subject matter of Article 25. It has, though, strongly implied that the ‘essence’ of Article 8 CFR requires adoption of ‘technical and organisational measures’ to ensure that personal data are given ‘effective protection’ against ‘risk of abuse and against any unlawful access and use’.\(^3\) This requirement is in line with the thrust of Article 25, particularly the provisions of Article 25(2) on data protection by default. The requirement suggests that data protection by design and by default is part of the EU’s constitutional fabric. This may have repercussions for how stringently the provisions of Article 25 (and, indeed, the equivalent provisions in the LED) are to be construed and applied.

Additionally, the CJEU has indirectly fostered the aims of Article 25 in some of its decisions dealing with internet mechanisms. A prime example is its judgment in the Google Spain case.\(^4\) While the Court did not require any substantial modification of the design of Google’s search engine, it did require Google (and other search engine operators) to reconfigure systemic aspects of search engine operations so that they are more privacy friendly.

The ECtHR has also embraced the ideals manifest in Article 25. Already in 2008, the Court issued a judgment holding that Finland violated Article 8 ECHR due to its failure to secure, through technological-organisational measures, the confidentiality of patient data at a public hospital.\(^5\) While Finnish law provides legal remedies for breaches of data confidentiality, this was judged insufficient in order for Finland to meet its positive obligations under Article 8: ‘What is required in this connection is practical and effective protection to exclude any possibility of unauthorised access occurring in the first place. Such protection was not given here’.\(^6\) Although the Court made no reference to ‘data protection by design and by default’ or closely linked notions, such as PbD, the basic thrust of its judgment necessitates adoption of a mindset and methods in line with these notions. Further, the above-cited paragraph of the Court’s judgment implies a requirement for data accessibility limits that, as a point of departure, guarantee confidentiality of data. This is akin to the requirement of data protection ‘by default’ in Article 25(2) GDPR. On the basis of this judgment, a solid argument can be made that data protection by design and by default is, in effect, an integral element of a state’s positive obligations to secure respect for private life pursuant to Article 8 ECHR, at least with respect to personal health data.

It is not unlikely that the CJEU would rule similarly with respect to the obligations flowing from Articles 7 and 8 CFR and Article 16 TFEU (independently of GDPR Article 25). This is particularly in light of the so-called homogeneity clause in Article 52(3) CFR together with CJEU recognition that Article 7 CFR ‘must … be given the same meaning and the same scope as Article 8(1) of the ECHR, as interpreted by the case-law of the European Court of Human Rights’.\(^7\)

\(^3\) Joined Cases C-293/12 and C-594/12, Digital Rights Ireland paras. 40 and 66; see also para. 67.
\(^4\) Case C-131/12, Google Spain.
\(^5\) ECtHR, I v Finland.
\(^6\) Ibid., para. 47.
\(^7\) Case C-400/10 PPU, J. McB, para. 53. For further elaboration, see Bygrave 2017B.
C. Analysis

The overall thrust of Article 25 is to impose a qualified duty on controllers to put in place technical and organisational measures that are designed to implement effectively the data protection principles of the GDPR and to integrate necessary safeguards into the processing of personal data so that the processing will meet the Regulation’s requirements and otherwise ensure protection of data subjects’ rights. The duty is a key element of the principle of accountability mentioned in Article 5(2) and developed in Article 24. The initial wording of the duty is similar to the initial wording of the duty under Article 32 to ensure adequate security of processing. Yet, unlike the latter, the duty under Article 25 expressly applies not just at the time of processing but also beforehand when the controller determines the means for processing – i.e., the stage of designing an information system. Moreover, it extends (in Article 25(2)) to ensuring – apparently without qualification – default application of particular data protection principles – most notably minimisation and proportionality – and default limits on data accessibility.

The duty imposed by Article 25(1) is qualified by an extensive list of contextual factors. These will be determined largely (but not exclusively) by the data protection impact assessment that controllers are required to conduct pursuant to Article 35. There is accordingly a link between impact assessments and Article 25 requirements. However, the requirement to undertake an impact assessment arises only where processing ‘is likely to result in a high risk’ to persons’ rights and freedoms (Article 35(1)), whereas the duty imposed by Article 25 does not. Nonetheless, the contextual factors listed at the start of Article 25(1) evidence a risk-based approach to assessing what measures are required.

In keeping with common conceptions of PbD, the measures referred to in Article 25 are not just technical but also organisational. In other words, they embrace not simply the design and operation of software or hardware; they extend to business strategies and other organisational practices as well, such as rules determining which and under what circumstances employees in an organisation are authorised to access or otherwise process particular categories of personal data. The reference to ‘pseudonymisation’ as an example of a suitable measure is supplemented by other examples listed in recital 78. At the same time, Article 25(1) stipulates that the measures concerned must be ‘designed to implement data-protection principles’. The latter denote primarily the principles listed in Article 5. This is confirmed by the reference to ‘data minimisation’ as an example (listed in Article 5(1)(c)). Whether Article 25(1) embraces other data-protection principles than those listed in Article 5 is a moot point and arguably of academic interest only, as the pith of such principles is adequately covered by Article 5, at least at an operational level. Further guidance on the parameters of Article 25 measures is expected to come from codes of conduct prepared by industry bodies (Article 40(2)(h)), from certification schemes (Article 25(3) in combination with Article 42), and from advice provided by data protection authorities.

There are significant differences between the ‘by design’ requirements of Article 25(1) and the ‘by default’ requirements of Article 25(2). First, the former cover a

---

8 See e.g. Cavoukian 2009.
potentially wider range of data protection measures than the latter, which focus on ensuring data minimisation and confidentiality. Secondly, the former appears to be largely process-oriented, while the latter are concerned with results that guarantee data minimisation and confidentiality, at least as a point of departure. The CJEU and ECtHR jurisprudence mentioned earlier buttresses the relatively absolutist orientation of Article 25(2) requirements, as does the omission from Article 25(2) of the various contextual qualifications that introduce the requirements of Article 25(1). However, it is arguable that these qualifications are to be read into the adjective ‘appropriate’ used to describe Article 25(2) measures. If they are, the latter are less absolutist than first appears.

As indicated above, Article 25(1) measures are to be taken at both the design stage and processing stage. The same necessarily applies for Article 25(2) measures even if Article 25(2) does not spell this out. On their face, both sets of measures are to be taken by controllers only. Controllers are basically defined as entities that determine or co-determine the purposes, conditions, and means of processing personal data (Article 4(7)). Whether and to what extent basic design decisions in information systems development will be taken by persons or organisations acting in a controller capacity are open questions. Article 25(1) formulates the design stage in terms of when the controller assumes controller status (‘the time of the determination of the means for processing’). This might not equate with the time when a particular data-processing device is actually designed and manufactured, thus undermining the goal of ensuring that privacy interests are fully integrated into information systems architecture. However, recital 78 brings PbD ideals to bear on actors other than controllers – namely, ‘producers’ of products, services and applications that involve processing of personal data. These actors are subject to less stringent requirements (‘should be encouraged’) than those imposed on controllers.

At the same time, Article 25 prevents, on its face, controllers from using technologies that collect more personal data than is strictly necessary for technological functionality or that ‘leak’ personal data to outsiders. This might shape the market and technology foundations for information systems development in a privacy-friendly direction. PbD ideals are also brought to bear on processors inasmuch as controllers are only permitted to use processors ‘providing sufficient guarantees to implement appropriate technical and organisational measures’ (Article 28(1)); see too recital 81). Thus, the Regulation evinces an expectation that the duty imposed by Article 25 on controllers will be passed both ‘downstream’ to processors and ‘upstream’ to technology developers.

The duty imposed by Article 25 plays a role in the application of numerous other GDPR provisions. For instance, in assessing whether processing of personal data for another purpose is compatible with the initial purpose for which the data is collected, account shall be taken of, inter alia, ‘the existence of appropriate safeguards, which may include encryption or pseudonymisation’ (Article 6(4)(e)). Further, the requirement imposed by Article 34 on a controller to communicate a personal data breach to the data subject may be relaxed if the controller ‘has implemented appropriate technical and organisational protection measures’ (Article 34(3)(a); see too recitals 87 and 88). Additionally, Article 83(2)(d) stipulates that in determining the imposition of fines for breach of the Regulation, ‘due regard’ shall be taken of, inter alia, ‘the degree of responsibility of the controller or processor taking into
account technical and organisational measures implemented by them’ pursuant to Article 25. Moreover, recital 78 states that the ‘principles of data protection by design and by default’ are to play a role in public procurement tenders: the principles ‘should … be taken into consideration’ in this context. The latter phrasing falls short of making data protection by design and by default a prerequisite for such tenders, but is otherwise ambiguous as to how much weight the principles should be given.

The provisions of Article 25 are replicated in Article 20 LED, albeit with two minor differences. One difference is that Article 20 omits reference to certification mechanisms. The other difference occurs in the elaboration of Article 20 in recital 53 where it is stated that the implementation of the measures referred to in Article 20 ‘should not depend solely on economic considerations’.
Select Bibliography

Academic writings


Papers of data protection authorities


Reports

Article 46

Transfers subject to appropriate safeguards

Prof. Christopher Kuner

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:
   (a) a legally binding and enforceable instrument between public authorities or bodies;
   (b) binding corporate rules in accordance with Article 47;
   (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
   (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
   (e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights; or
   (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:
   (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
   (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.
Relevant recitals

(108) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.

(109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

(114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that they will continue to benefit from fundamental rights and safeguards.

CLOSELY RELATED PROVISIONS

Recital 6 (facilitate transfer to third countries while ensuring a high level of protection); 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 15(2) (right to access information about appropriate safeguards pursuant to Article 46); 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); Articles 30(1)(e) and 30(2)(c) (internal records about data transfers); Article 40(2)(j) (data transfer codes of conduct); Article 40(3) (adherence to data transfer codes of conduct by controllers and processors not subject to the Regulation); Article 42(2) (adherence to data transfer certifications by
controllers and processors not subject to the Regulation); Article 58(3)(g) and (h) (powers of supervisory authorities to adopt standard contractual clauses and authorise contractual clauses); Article 64(1)(d) and (e) (opinion of the Board regarding determination of standard data protection clauses and authorisation of contractual clauses); Article 83(5)(c) (fines for non-compliance with data transfer restrictions)

RELATED ARTICLES IN LED [Directive (EU) 2016/680]

Recital 36 (obligation of information about specific conditions applicable to the data processing by a competent authority to the data recipients in third countries); Article 37 (transfers subject to appropriate safeguards) (see too recital 71)

RELEVANT CASE LAW

CJEU

Case C-362/14, Maximillian Schrems v Data Protection Commissioner, judgment of 6 October 2015 (ECLI:EU:C:2015:650).
A. Rationale and Policy Underpinnings

Article 46 GDPR provides that when an adequacy decision has not been issued under Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if it has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available. Such appropriate safeguards are based not on a detailed evaluation of the legal system of the country to which the data are to be transferred, as is the case when an adequacy decision has been issued, but are a set of protections that apply to the particular data transfer. The rules of Article 46 build and expand on those of Article 26 DPD. The multi-tiered structure of Chapter V means that if an adequacy decision has been issued then that should be relied on; if not, then appropriate safeguards should be used.

B. Legal Antecedents

1. EU legislation

Article 26(2) DPD provided that data transfers may be carried out absent adequate protection in the third country to which personal data are transferred ‘where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses’. The GDPR maintains and expands the concept of adequate safeguards, which it renames ‘appropriate safeguards’.

Under the DPD, two main types of ‘adequate safeguards’ were recognized, namely contractual clauses and binding corporate rules (BCRs). BCRs were recognized de facto by supervisory authorities under the DPD because they were not mentioned explicitly in it.¹ Contractual clauses are concluded between the data exporter in the EU and the data importer outside the EU to whom the data are sent and contain obligations on each to provide certain protections to the personal data. They can either be ‘standard contractual clauses’, the text of which is standardized and adopted by a formal decision of the European Commission, or ‘ad hoc’ clauses that are drafted in each specific case and must be approved by the DPAs before use.² Article 46 introduces some new types of appropriate safeguards, which are discussed later on and which were not included in the DPD.

In practice, standard contractual clauses have proved to be the most important type of adequate safeguards under the DPD. The history of the standard contractual clauses began in 1992, when the Council of Europe, European Commission, and International Chamber of Commerce (ICC) jointly approved a set of model clauses for international data transfers.³ While this contract was never formally approved by the Commission as model clauses for the transfer of personal data outside the EU, it served as inspiration for later work to draft model clauses. In 2001, the Commission then

---

¹ See the discussion of Art. 47.
² See regarding the use of contractual clauses under the DPD, Kuner 2007, pp. 191-210; Kuner 2013, pp. 43-44.
approved a set of standard contractual clauses for controller to controller transfers, and a set of standard contractual clauses for controller to processor transfers on 27 December 2001. Following criticism of the standard clauses, the Commission then entered into consultations with a coalition of various business groups led by the ICC and approved an alternative set of controller to controller clauses in 2004, and an alternative set of controller to processor clauses in 2010. The 2004 controller to controller clauses apply in addition to those adopted in 2001 (i.e., either set can be used for controller to controller transfers), while the 2010 controller to processor clauses replace those adopted earlier (i.e. the 2001 controller to processor clauses were repealed by the 2010 set).

In 2016 the Commission adopted a decision amending the 2001 controller to controller clauses and the 2010 controller to processor clauses to take into account the Schrems judgment of the CJEU. However, this decision of 2016 does not make reference to the third standard clauses decision that is still in force (Commission Decision 2004/915). Perhaps this was thought unnecessary since Decision 2004/915 merely amends Decision 2001/497, but one would have thought that some reference would have been made to the 2004 decision, if only to note that it amended the earlier 2001 decision, particularly since the 2004 decision includes a new set of model clauses in the Annex.

2. National legislation

All Member States implemented Article 26 DPD.

Under the DPD, approval of adequate safeguards by the competent data protection authority (DPA) was required in a number of Member States, particularly for ad hoc contractual clauses and BCRs. This will no longer be the case with regard to use of standard contractual clauses approved either by the Commission alone (Article 46(2)(c)) or adopted by a DPA and then approved by the Commission (Article 46(2)(d)). Approval of custom-drafted (ad hoc) contractual clauses by the competent DPA is still required under the GDPR (Article 46(3)), with its determination subject to the consistency mechanism referred to in Article 63 (Article 46(4) GDPR). The competent DPA is determined under Article 55. Adoption by the Commission of standard contractual clauses, and approval by the Commission of standard clauses adopted by DPAs, are both carried out under the examination procedure referred to in Article 93(3) (Articles 46(2)(e)-(d) GDPR). Adoption by a DPA of its own standard

---

6 The author led negotiations on behalf of the ICC and the business groups.
9 See Ibid., rec. 25, stating that ‘Decision 2002/16/EC should be repealed’.
10 Case C-362/14, Schrems. See the discussion of Art. 45 for a detailed explanation of the judgment.
11 EC Standard Contractual Clauses Processors 2016. The 2016 decision replaces Art. 4 of each of the two sets of clauses with the following text: ‘Whenever the competent authorities in Member States exercise their powers (…) leading to the suspension or definitive ban of data flows to third countries in order to protect individuals with regard to the processing of their personal data, the Member State concerned shall, without delay, inform the Commission, which will forward the information to the other Member States.’
contractual clauses or of ad hoc contractual clauses requires an opinion of the European Data Protection Board (Article 64(1)(d)-(e)).

3. Case law

There are no judgments of the CJEU or the European Court of Human Rights dealing with the subject matter of Article 46. However, on 12 April 2018 the Irish High Court referred to the CJEU a series of questions that could put into question the use of standard contractual clauses to transfer personal data; the final referral had not yet been published by the CJEU at the time this text was finalized.

C. Analysis

1. Status

The use of appropriate safeguards allows the transfer of personal data when no adequacy decision has been issued by the Commission regarding a country or international organisation (including a territory or one or more specified sectors within that third country as specified in the decision). The GDPR does not contain a concise definition of ‘appropriate safeguards’, but does describe them as follows in recital 108:

Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default.

Appropriate safeguards are to be regarded as more limited in scope than an adequacy decision, which is issued based on the totality of conditions in the third country or international organisation, including such factors as the rule of law, respect for human rights, and other factors that relate to the legal system as a whole. By contrast, appropriate safeguards are tailored to particular transfers or types of transfers, and thus are narrower in scope than the protection granted with regard to countries and international organisations for which adequacy decisions have been issued.

Thus, appropriate safeguards cannot provide protection against certain data protection risks that must be taken into account when an adequacy decision is issued (e.g., access to the data by public authorities in the country to which the data are transferred, as provided for in Article 45(2) GDPR).

The list of appropriate safeguards provided for in Article 46 seems not to be exclusive (this follows from the words ‘may be provided for’). As recital 109 makes clear, this means that nothing in the GDPR prevents the parties to a data transfer from providing extra protection beyond what the GDPR requires, so that its provisions regarding data

---

13 Maximilian Schrems, Irish High Court, 2016 No. 4809 P.
transfers should be seen as a floor rather than a ceiling. Recital 114 also invites parties involved in data transfers to make use of innovative solutions to protect them beyond those solutions listed in the GDPR.\textsuperscript{14}

The key criterion to keep in mind when designing additional safeguards is that they should provide ‘enforceable data subject rights and effective legal remedies for data subjects’ (Article 46(1) GDPR). Recital 108 also states that any appropriate safeguards ‘should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default’, which may refer to the principles of Article 5 GDPR.

2. Harmonisation

Under the principle of the primacy of EU law over national law,\textsuperscript{15} data transfers under national systems that do not comply with the requirements of Article 46 will no longer be allowed. Thus, for example, the UK system whereby parties transferring personal data are able to determine on their own whether the contractual clauses they put in place provide sufficient safeguards, with the UK Information Commissioner refusing to review them or issue authorisation of such transfers absent ‘exceptional circumstances’,\textsuperscript{16} would no longer seem to be tenable, given the requirement in Article 46(3)(a) that ad hoc contractual clauses must be authorised by the competent DPA.

The new regime for appropriate safeguards under Article 46 will cure the fragmented legal situation that existed under Article 26 DPD, under which, for example, some DPAs required authorisation of use of the Commission-approved standard contractual clauses and some did not. Article 46(2) GDPR provides that the following forms of appropriate safeguards do not require further authorisation by a DPA: ‘a legally binding and enforceable instrument between public authorities or bodies’; binding corporate rules; standard contractual clauses adopted by the Commission; standard clauses adopted by a DPA and approved by the Commission; approved codes of conduct; and approved certification mechanisms. Under Article 46(2), standard contractual clauses are adopted by the Commission and standard clauses adopted by a DPA are approved by the Commission pursuant to the examination procedure under Article 93(2), which refers to Article 5 of the so-called Comitology Regulation.\textsuperscript{17}

However, under Article 46(3), other appropriate safeguards do require DPA authorisation. This includes other types of contractual clauses, and provisions to be inserted into administrative arrangements between public authorities, authorisation for both of which must be obtained based on the consistency mechanism under Article 63 GDPR.

Some Member States have imposed formal requirements on the use of appropriate safeguards such as contractual clauses; for example, some of them have required that the signatures of data exporters and data importers to standard contractual clauses be

\textsuperscript{14} See also rec. 113, stating ‘Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses’.

\textsuperscript{15} See Rosas and Armati 2012, p. 15.

\textsuperscript{16} See UK Information Commissioner 2017.

\textsuperscript{17} Regulation (EU) No 182/2011.
notarized, which may in some cases require that an ‘apostille’ be affixed to the clauses under the Hague Convention Abolishing the Requirements of Legalisation for Foreign Public Documents.\(^\text{18}\) Such requirements may remain applicable after entry into force of the GDPR even with regard to those appropriate safeguards described in Article 46(2), since they relate to the technicalities of the signature of the clauses, and not to specific authorization by the DPAs.

3. Other requirements

It is important to remember that the ability to transfer personal data based on appropriate safeguards is subject to compliance with all other requirements for data processing besides those concerning international data transfers (this follows from Article 44).

This includes in particular, but not exclusively, provisions of the GDPR specifically relevant to international data transfers under Article 46, for example the obligation to inform data subjects that data are to be transferred internationally (Articles 13(1)(e)-(f), Articles 14(1)(e)-(f), Article 15(1)(c), and Article 15(2)); duties of data processors (Article 28(3)(a)); and the obligation to keep records concerning data processing (Articles 30(1)(d)-(e) and Article 30(2)(c)). Also, contractual clauses to transfer personal data under Article 46 should not be confused with contractual clauses mentioned in the GDPR to be used for other purposes (e.g., Article 28(3) GDPR, which requires that processing by a data processor be carried out based on a written contract).

4. Prior authorisations

Under Article 46(5) GDPR, authorisations issued by a Member State or supervisory authority on the basis of Article 26(2) DPD (such as regarding ad hoc contractual clauses or BCRs) remain in effect, as do decisions adopted by the Commission on the basis of Article 26(4) DPD (such as concerning standard contractual clauses). Thus, data transfers may continue to be carried out under such instruments. The competent DPA may amend, replace, or repeal authorisations granted on the bases of Article 26(2) DPD, but does not have to, just as the Commission may (but need not) amend, replace, or repeal decisions it adopted under Article 26(4) DPD. Any amendment, replacement, or repeal of Commission decisions must be carried out in accordance with the examination procedure referred to in Article 93(2) (as provided in Article 46(2)). Unlike the case with adequacy decisions under Article 45(3) there is no requirement for periodic review of the standard contractual clauses, but it can be expected that the Commission will in time adopt new sets of them to replace those approved under the DPD, and possibly also clauses dealing with further data procession situations (such as with regard to processor-to-processor transfers).

5. Practical questions

The GDPR does not contain requirements as to how contractual clauses, whether standard or otherwise, should be signed, beyond stating that parties may include contractual clauses ‘in a wider contract, such as a contract between the processor and

---

\(^\text{18}\) Hague Convention on the legalisation of documents.
another processor...’ (recital 109). This gives the parties considerable latitude in determining how to implement them in practice, e.g., by signing them separately, incorporating them into an existing contract, or otherwise.

Parties may attempt to organise their signature of contractual clauses (whether the standard ones or otherwise) based on their corporate structure. For example, if Company A and Company B are both data exporters in the EU, and Company B is a subsidiary of Company A, then the question may arise as to whether Company A may sign the clauses as a data exporter also on behalf of Company B. Furthermore, the question may also arise as to whether Company B may grant a power of attorney (POA) to Company A to sign on its behalf. Similar questions may arise with regard to signature of the clauses by data importers.

Signature of the clauses is based on a party’s status either as a data exporter or a data importer, and not on its particular status under company or corporate law. Thus, the fact that Company B may be a subsidiary of Company A is not relevant with regard to signature of the clauses: if Company A and Company B are both data controllers, then they should both sign the clauses, and Company A may not sign on Company B’s behalf merely because it stands higher in the corporate hierarchy. In such a situation it could be possible for Company B to grant a power of attorney to Company A and thus have it sign on Company B’s behalf. However, the granting of powers of attorney is often fraught with difficulties under company law, particularly when the party to which a power of attorney is given is located outside the EU.

It can be difficult to decide which set of clauses to use (controller to controller or controller to processor), since it is not always clear whether the data importer is a controller or a processor. Parties signing the clauses will have to use their best judgment in deciding which types of clauses to use, based on the characterization of the parties as data controllers or data processors under the GDPR.19

While the WP29 has issued a draft opinion on a proposed set of ad hoc contractual clauses for data transfers from EU data processors to non-EU sub processors, 20 this has not yet been officially approved by the Commission. However, recital 109 states that ‘The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor...’ Thus, parties may consider using one of the sets of standard contractual clauses in a processor-to-processor scenario as well.

The Commission-approved standard contractual clauses may not be amended in any way (i.e., they must be adopted verbatim), 21 aside from filling out the annexes. In practice, any amendment of the standard clauses means that they will considered to be ad hoc clauses that will require the authorization of the competent DPA. However, the GDPR makes it clear that there is no prohibition against ‘adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the

19 See the definition of these terms under Art. 4 GDPR.
20 See WP29 2014.
21 See, e.g., EC Standard Contractual Clauses 2004, rec. 3, stating that ‘data exporters should not, however, be allowed to amend these sets or totally or partially merge them in any manner’. 
standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects’ (recital 109). Additional clauses are to be recommended in cases involving data transfers where there is a particularly high risk or sensitivity.

6. New forms of appropriate safeguards: legally binding and enforceable instruments, codes of conduct, certification mechanisms, and provisions inserted into administrative arrangements

Article 46 also adds new forms of appropriate safeguards for the transfer of personal data beyond those contained in the DPD, namely the following: ‘a legally binding and enforceable instrument between public authorities or bodies’ (Article 46(2)(a)); ‘an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights’ (Article 46(2)(e)); ‘an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights’ (Article 46(2)(f)); and ‘provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights’ (Article 46(3)(b)). Each one of these will now be considered in turn.

The reference to ‘a legally binding and enforceable instrument between public authorities or bodies’ (Article 46(2)(a)) allows data transfers based on enforceable legal instruments (such as contractual clauses) between public authorities or bodies in the EU and those in third countries. This could include, for example, an agreement to share data between an EU-based public authority and one in a third country. Under Article 46(2), no DPA authorisation is required for the use of such an instrument.

The reference to ‘an approved code of conduct’ refers to a code drawn up by ‘associations or other bodies’ pursuant to Article 40. The GDPR does not contain a definition of ‘code of conduct’. That article contains a detailed list of provisions that a code of conduct must contain and how it must be adopted and implemented. Under Article 40(5), such a code must be approved by the competent DPA as determined by Article 55, which is confirmed by Article 46(2)(e) (referring to ‘an approved code of conduct’); however, no further authorisation is required (Article 46(2)). Use of a code of conduct to transfer data requires ‘binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights’ (Article 46(2)(e)), indicating that it must be legally binding between the parties that have adopted it (for example, on a contractual level). The Commission may issue implementing acts finding that approved codes of conduct have general validity within the EU (Article 40(9)), though the GDPR does not explain what ‘general validity’ means in a legal sense (e.g., whether adherence to an approved code of conduct would lead to a presumption of compliance with the GDPR’s provisions on international data transfers).

---

22 See also Art. 40(2)(j) GDPR, listing one of the potential purposes for a code of conduct as ‘the transfer of personal data to third countries or international organisations’.

*Kuner*
The Commission may also approve as having general validity codes of conduct adhered to by data controllers and data processors not subject to the GDPR (Article 40(3)); this could presumably include, for example, a trade association in a third country whose members are not subject to the GDPR but who want to make it easier for EU business partners to transfer personal data to them. Article 40(3) states that by having such a code approved under Article 40(5) and having it declared as having general validity under Article 40(9), such third country organizations would be providing ‘appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2)’. However, Article 46(1) refers to appropriate safeguards that are provided by the data controller or data processor transferring personal data from the EU, not by the parties receiving the data, which seems to present a contradiction with Article 40(3). Even though this provision is explicitly designed to apply to data controllers and data processors not subject to the GDPR, once the relevant organizations adopt such a code they would be subject to the ‘binding and enforceable commitments’ (Article 40(3)) under the GDPR that they have to assume in order for the code to be approved.

The reference to ‘an approved certification mechanism’ means a certification mechanism adopted pursuant to Article 42. The GDPR does not contain a definition of ‘certification mechanism’, though it does mention them in the same breath as ‘data protection seals and marks’ (Article 42(1)). An example of a certification mechanism would thus presumably be a trustmark placed on a web site, which would have to be backed up by some sort of code of conduct or code of practice; the GDPR does not address the interaction of certification mechanisms with codes of conduct, though presumably if they were to be used together then both would have to be approved under the relevant provisions of the GDPR. Certification mechanisms are voluntary, but under Article 42(5) may be approved either by a DPA or a national certification body as set out in Article 43. A certification mechanism must contain ‘binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights’ (Article 46(2)(f)), and must thus be legally binding. Under Article 46(2), no additional DPA authorisation is required for the use of a certification mechanism as providing adequate safeguards once it has been approved as provided in Article 46(2)(f). According to Article 42(5), a ‘common certification, the European Data Protection Seal’ may ‘result’ from criteria approved by the EDPB, but it is unclear whether this would have any legal effect with regard to international data transfers.

As is the case with codes of conduct (see above), data protection certification mechanisms may be established for data controllers and data processors not subject to the GDPR (Article 42(2)); this could presumably include, for example, a trade association in a third country whose members are not subject to the GDPR but who want to make it easier for EU business partners to transfer personal data to them. Such certification mechanisms may ‘be established for the purpose of demonstrating the existence of appropriate safeguards … under the terms referred to in point (f) of Article 46(2)’ (Article 42(2)). Such a certification mechanism has to be approved either by a certification authority under Article 43 or a DPA (Article 42(5)). Article 46(1) refers to appropriate safeguards that are provided by the data controller or data processor transferring personal data from the EU, not by the parties receiving the data, which seems to present a contradiction with Article 42(2). Even though this provision
is explicitly designed to apply to data controllers and data processors not subject to the GDPR, once the relevant organizations adopt such a certification mechanism they would be subject to the ‘binding and enforceable commitments’ (Article 42(2)) under the GDPR that they have to assume in order for it to be approved.

Finally, Article 46(3)(b) allows data transfers based on ‘provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights’. These arrangements are presumed not to be legally binding (see the statement in recital 108 that ‘authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding’), which is how such arrangements are to be distinguished from the ‘legally binding and enforceable instrument between public authorities or bodies’ referred to in Article 46(2)(a). The types of arrangements foreseen in Article 46(3)(b) could include, for example, a memorandum of understanding between public authorities or bodies, as long as they provide for enforceable and effective rights for data subjects (recital 108 GDPR). Data transfers based on such administrative arrangements require authorisation from the competent DPA in accordance with the examination procedure referred to in Article 93(2) (as provided in Article 46(3)).

### 7. Enforcement

Under the CJEU’s Schrems judgment, an individual must be able to make a claim to a DPA contesting the compatibility of data transfers based on an adequacy decision with the protection of privacy and fundamental rights, and the DPA must examine the claim with all due diligence. If the DPA rejects the claim, the individual must have access to judicial remedies allowing him to contest this decision before national courts, and the courts must stay proceedings and make a reference to the Court for a preliminary ruling. If the DPA finds such claim to be well-founded, it must be able to engage in legal proceedings based on national legislation to enable the courts to make a reference for a preliminary ruling concerning the decision’s validity. Given the high value that the CJEU has set on the fundamental right to data protection, these requirements should apply to appropriate safeguards under the GDPR as well.

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 organization, 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.

Infringements of Article 46 are subject to the higher level of administrative fines under Article 83(5)(c), i.e., up to 20,000,000.00 Euros or 4% of the total worldwide turnover of the preceding financial year, whichever is higher.

It should also be noted that the LED also allows data transfers to be carried out based on appropriate safeguards in the area of law enforcement, which is outside the scope
of the GDPR.\textsuperscript{23} Article 37(1) LED mentions two types of appropriate safeguards, namely ‘appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or (b) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with regard to the protection of personal data.’ Data transfers carried out under (b) require that the DPA be informed and that certain documentation about the transfer must be kept and made available to the DPA upon request; these seem to provide less protection than the specific safeguards mentioned in Article 46(3)(b) GDPR, which refers to “enforceable and effective data subject rights”.

\textsuperscript{23} See Art. 2(2)(d) GDPR.
Select Bibliography

Legislation


Case law


Academic writings


Simitis and Dammann, EU-Datenschutzrichtlinie (Nomos Verlag 1997).

Papers of data protection authorities


Others

Article 56

Competence of the lead supervisory authority

Dr. Hielke Hijmans

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Relevant recitals

(124) Where the 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, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are...
substantially affected, or because a complaint has been lodged with them. Also, where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection.

(125) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.

(126) The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.

(127) Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorities concerned ('one-stop-shop mechanism'), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision vis-à-vis the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.

(128) The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the
supervisory authority of the Member State where the public authority or private body is established.

CLOSELY RELATED PROVISIONS

Article 4 (16) (Definition of main establishment); Article 4 (22) (Definition of supervisory authority concerned); Article 4 (23) Definition of cross border processing); Article 57(Tasks) (see too recitals 122, 123, 132, 133) Article 58 (Powers) (see too recital 129); Article 59 (Activity reports); Articles 60-67 (Chapter VII, Cooperation and Consistency, Sections 1 and 2) (see also recitals 126, 130-138)

RELEVANT CASE LAW

CJEU

Case C-131/12, Google Spain v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014 (ECLI:EU:C:2014:317).
Case C-362/14, Maximillian Schrems v Data Protection Commissioner, judgment of 6 October 2015 (ECLI:EU:C:2015:650).
Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (pending).
A. Rationale and Policy Underpinnings

Article 56 GDPR lays down the foundation of possibly the most significant novelty of the GDPR, the mechanism of enforcement for the cross-border processing within the EU. This mechanism is construed around a lead supervisory authority cooperating with other concerned authorities in a ‘one stop shop mechanism’ in an endeavour to reach consensus. The mechanism must lead to one single enforcement decision with EU wide applicability, without however centralising enforcement with a supervisory authority at EU level. This mechanism must reconcile the need for a level playing field within the EU – which requires consistent enforcement within the EU - with the concepts of proximity with decision making close to the citizen\(^1\) and of executive federalism.\(^2\)

This objective, aimed at satisfying the need for both the consistency of enforcement and for justified demands for national treatment, is not just a feature of the mechanism itself, but is also reflected in the derogation in Article 56 (2) GDPR. This clause is designed to ensure the competence of local supervisory authorities to handle complaints of individuals with a local nature and to deal with subject matter relating only to establishments of organisations within the national borders.

The one stop shop mechanism with a lead authority is established by Article 56 and elaborated in Article 60. It ensures that controllers and processors with multiple establishments in the EU or whose activities substantially affect data subjects in multiple Member states have one single supervisory authority (DPA) as their sole interlocutor. This is the lead DPA, which also takes the final decision in respect of the processing by this controller or processor. However, this single interlocutor does not have exclusive competence in the course of the process; it has the lead role in a cooperative process.

A further rationale of the article is the need for effectiveness. Procedural rules are inserted in Article 56 (3), (4) and (5), to avoid legal uncertainty about the application of the derogation to the one stop shop mechanism.

B. Legal Antecedents

1. EU legislation

Article 56 GDPR is a novelty within EU data protection law. However, the need for reconciling consistent enforcement within the EU with the competences of national authorities is also apparent in other areas of EU law, although the models for cross border enforcement are different.

The enforcement of EU competition law and in particular the regime of Regulation 1/2003\(^3\) is the most obvious example. This regulation facilitates the cooperation of the enforcement bodies at EU level and at national level. Unlike the area of data protection, a centralised EU enforcement body exists (the European Commission itself), but the system is also characterised by decentralised enforcement. National

\(^1\) Legal Service Contribution.
\(^2\) See on executive federalism, Lenaerts and van Nuffel 2011, at 17-002.
\(^3\) Council Regulation 1/2003.
competition authorities are competent to supervise infringements of EU competition law. These national competition authorities cooperate with each other and with the European Commission in a European Network of Competition Authorities.\textsuperscript{4}

A different model may be found in the sector of electronic communications,\textsuperscript{5} a sector with links to data protection.\textsuperscript{6} National regulatory authorities (NRAs) are responsible for enforcing the EU regulatory framework for electronic communications. However, they are obliged to cooperate with each other (and with the Commission) in the Body of European Regulators for Electronic Communications (BEREC). NRAs and the Commission have to take the utmost account of any opinion, recommendation, guidelines, advice or regulatory best practice adopted by BEREC.\textsuperscript{7}

Further models of (enforcement) cooperation between authorities (agencies) of Member States in an EU framework exist in a variety of sectors, such as the supervision of financial markets.\textsuperscript{8}

2. \textit{International treaties}

The subject matter of Article 56 GDPR is not dealt with in any international treaty. The additional protocol to the Convention 108 of the Council of Europe, adopted in 2001\textsuperscript{9} only provides that the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

3. \textit{National legislation}

The German Federal Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 contains arrangements to align the federal system of Germany - in many cases a DPA of a Land is competent and not the Federal German DPA – with the GDPR.\textsuperscript{10} The act contains a provision on the lead supervisory authority of a Land in the one-stop-shop mechanism pursuant to the GDPR, as well as a mechanism in cases where complaints are lodged in Germany with a DPA which is not the lead authority. It also contains a procedure in case there is no agreement on determining the lead authority. Finally, it defines how the German DPAs establish a common position, also vis-à-vis the lead DPA in another EU Member State.

\begin{itemize}
\item \textsuperscript{4} Lenaerts and van Nuffel 2011, at 11-013.
\item \textsuperscript{5} BEREC Regulation.
\item \textsuperscript{6} Notably because of the EPD. This directive allows Member States to assign enforcement tasks to national regulators for electronic communications.
\item \textsuperscript{7} BEREC Website.
\item \textsuperscript{8} Ottow 2014.
\item \textsuperscript{9} Article 1 (5) Additional Protocol Convention 108.
\item \textsuperscript{10} German GDPR Implementation Law, at paras 18-19.
\end{itemize}
C. Analysis

1. The concept of the lead supervisory authority: a primus inter pares?

As a rule, DPAs are competent on their national territory, but this competence is no longer exclusive in situations of cross border processing. Article 56(1) contains an exception to this rule which is founded on notions of territorial competence under public international law. As a result of the one-stop-shop mechanism, the DPA of the country of main or single establishment is, in those situations, leading the enforcement by all concerned DPAs.\(^{11}\) The Article 29 Working Party (WP29) underlines that the task consists of coordinating investigations.\(^{12}\)

The legislative history illustrates the concept well. The 2012 Commission Proposal contained a different concept. In cases of cross border processing only one DPA would be competent. However, this competence was an exclusive competence, not a competence to lead/coordinate an enforcement action. This exclusive competence was strongly criticised, precisely because it did not lead to a system of structural DPA cooperation.\(^{13}\)

The Commission proposal was simple. One DPA is competent. The proposal followed the logic of the internal market and is based on the principle of mutual recognition. A Member State should, normally, recognise decisions taken in other Member States. This principle also applies in other areas of EU law, particularly in the area of freedom, security and justice.\(^{14}\) The proposal provided one safeguard enabling other DPAs to get involved: before taking a decision the competent DPA should notify the EDPB, which could trigger the consistency mechanism on request of another DPA or the Commission.\(^{15}\) This safeguard could be characterized as a sort of emergency break, aiming at ensuring a consistent enforcement of EU data protection law.

This mechanism was not considered robust enough to prevent a single DPA from acting without considering the views of the DPAs in countries where individuals are affected. As noted by the Presidency of the Council: the ‘lead authority cannot adopt a “go-it-alone” attitude but needs to cooperate […]’.\(^{16}\) This position is based on the view that any DPA should be in a position to effectively protect individuals within its country; this role cannot be performed by or delegated to a DPA in another Member State.\(^{17}\)

As a result, Articles 56(1) and 60 ensure that the DPA of the Member State where the controller or processor has its main or single establishment in the EU cannot act alone. This DPA must take account of relevant and reasoned objections of concerned DPAs.\(^{18}\) If the DPAs do not agree on the outcome, the dispute resolution mechanism of Article 65 is triggered.

---

\(^{11}\) A ‘collaborative competence’, see Giurgiu et al. 2016, p. 348.
\(^{12}\) WP29 2017, p. 4.
\(^{14}\) E.g. Arts. 81 (1) and 82 (1) TFEU.
\(^{15}\) Art. 58 and rec. 97 and 98 GDPR Proposal.
\(^{16}\) Council Interinstitutional File One-Stop, p. 4
\(^{17}\) This is linked to proximity, discussed under 4 in this article.
\(^{18}\) Art. 60 (4).
The concept of ‘leading’ should be understood mainly as a procedural role. The lead DPA is responsible for the procedure and it drafts the enforcement decisions. However, at the end of the day, its position on substance is no stronger than that of any other DPA. Cooperation should take place ‘in an endeavour to reach consensus’.19

The term ‘primus inter pares’ may nevertheless be used. The lead DPA drafts the decision, takes the decision and defends the decision before the judiciary, where relevant. Moreover, it acts as the ‘sole interlocutor’ of the controller or processor.20 This gives the lead DPA at least an information position which is stronger than that of the other DPAs. In short, all DPAs are equal but the lead DPA is more equal than the others.21

2. The scope of application of Article 56(1)

The competence of a lead DPA is limited to situations of cross border processing, as defined in Article 4(23). Cross border processing includes two types of situations. The processing of personal data must take place in the context of activities of establishments of the controller or processor in more than one Member State. This requires that the controller (or processor) has establishments in more than one Member State. Alternatively, when the processing only relates to the establishment in one Member State, it is required that the processing substantially affects or is likely to substantially affect data subjects in multiple Member States.

This definition has two clear limitations. First, the exception to the exclusive competence of a DPA on its national territory does not apply when the processing of personal data takes place in the context of public tasks. Within this context, the DPA remains exclusively competent on its own territory, as a result of Article 55(2).22 Article 55(2) could lead to complexity. Imagine the provider of telecommunications services who stores the same communications data for commercial purposes – such as billing – and for the purpose of access by law enforcement authorities. This provider deals with a lead DPA (because of the commercial purpose) and with one or more local DPAs (because of the law enforcement purpose).

Second, there must be an establishment within the EU. As confirmed by the WP29, organisations without any establishment in the EU – whose activities fall within the scope of the GDPR on the basis of Article 3(2) - must deal with local DPAs in every Member State.23

However, it is not clear if an organisation with an establishment in the EU can have a lead authority also for processing activities which are conducted in the context of an establishment in a third country. 24 An argument in favour of the position that in many situations there can be a lead DPA can be drawn from the CJEU’s ruling in Google

---

19 Art. 60 (1).
20 Art. 56 (6).
21 To adapt the famous quote in George Orwell’s ‘Animal Farm’.
22 See the discussion of Art. 55 (2).
23 WP29 2017, p. 10. See also Jay 2017, at 21-018.
24 This point is addressed in CIPL 2016A, p. 6. The Centre asks for guidance.
Spain and Google$^{25}$ where the CJEU broadly interpreted the notion ‘in the context of the activities of an establishment’. Following this ruling, in many cases processing activities can be attributed to an establishment in the EU.

At the time of writing, it is equally unclear to what extent an organisation with an establishment within a country of the European Economic Area, but not in the EU itself, can benefit from a lead authority in Norway, Iceland or Liechtenstein. The agreement between the EU and these three countries on the applicability of the GDPR in those countries should have a specific provision to make this happen.$^{27}$

Article 56(1) is drafted with the example of businesses in mind.$^{28}$ The guidance of the WP29 also seems to mainly address multinational companies.$^{29}$ However, the GDPR does not exclude that the mechanism also applies to non-for-profit organisations which have establishments in more than one Member State.

3. The identification of the lead supervisory authority

Article 56(1) provides that in certain situations, there shall be a competent lead DPA. This lead DPA shall be the authority of the single or main establishment.

It is clear from the text of the GDPR that the competence of the lead DPA follows directly from the law and is not based on a constitutive decision of any administrative body. The only procedural rule in the GDPR relates to a situation “where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment”.$^{30}$

The GDPR, however, is silent about the identification of the lead DPA. This is an omission of the legislator since, in view of the wide range of organisational models of companies, it is often not evident what DPA will be the lead DPA. This already starts with the definition of main establishment in Article 4(16), with its key notion of the establishment where decisions on the ‘purposes and means of processing’ are taken. Given the wide variety of organisational models of companies, it is often not evident what entity within a company has the say over personal data processing. There are many situations where the central administration does not have the final say. There are also situations where companies provide a certain service in one establishment and another service in an establishment in another Member State. Does such a company only deal with one DPA? To give an even more complicated practical example, how may the lead DPA be identified in the situation of groups of companies operating in multiple Member States, where the organisation comprises both controller(s) and processor(s)?$^{31}$

---

$^{25}$ Case C-131/12, Google Spain, at para 60.
$^{26}$ See, e.g. Gömann 2017, at 2.1.1. See also: and Brkan 2016, p. 327.
$^{27}$ According to the website of the EFTA, a draft Joint Committee Decision (JCD) is under consideration by the EU and the three EFTA States with the aim of being incorporated into the EEA Agreement on 1 June 2018, see EFTA GDPR. The text of the underlying provisions is not publicly available.
$^{28}$ Legal Service Contribution, pp. 4-5.
$^{29}$ WP29 2017, p. 5.
$^{30}$ Art. 65(1)(b).
$^{31}$ Example from Centre for Information Policy Leadership, CIPL 2016A, p.4.
The WP29 guidance takes as a starting point that in situations which are not clear cut the controller or processor itself should designate its main establishment. However, the organisation does not have a final say on this, since the GDPR does not permit forum shopping, which would mean in this context choosing the DPA with the perceived most agreeable enforcement policy. This does not mean that an organisation is precluded from having a preference for a specific lead DPA, for instance because of language, likely size and resources, as well as regulatory approaches. In this case the organisation should adapt its operations in line with the GDPR. An example is an organisation ensuring the effective control of the processing activities in a specific Member State, for reasons relating to its preference for a specific lead DPA.

It is safe to say that the GDPR does not provide legal certainty. This is recognised by the Centre for Information Policy Leadership (CIPL) which has suggested a procedure for organisations to register with the lead DPA. Such a procedure is, however, not foreseen in the GDPR.

4. Article 56(2): Subject matter of a local nature

Whilst Article 56(1) is an exception to the territorial competence of a DPA, Article 56(2) creates an exception to the exception which restores the competence of the local DPA in certain limited cases of cross border processing. Local cases, although falling within the definition of cross border processing, should be treated locally. Recital 127 mentions as an example of a local case ‘where the subject matter concerns the processing of employees’ personal data in the specific employment context of a Member State’.

This exception to the exception was included in the GDPR after discussions in the Council and relates to the concept of proximity, an important aspect of the protection of individual rights. These discussions referred to proximity to the data subject as requiring a role of the local supervisory authority. They also mentioned that a local supervisory authority should treat ‘local cases’.

However, the result laid down in Article 56(2) is ambiguous. The applicability of this exception does not interfere with the mechanism where the relevant controller or processor deals with a lead DPA as its sole interlocutor. Moreover, although this paragraph states that the local DPA is competent to deal with subject matters of a local nature, the following paragraph empowers the lead DPA to decide whether this competence can be used in a specific case. It is also remarkable that a possible disagreement on competence between the local DPA and the lead DPA is not an issue which can lead to dispute resolution by the EDPB under Article 65(1). Of course, the local DPA can always ask for an opinion of the EDPB under Article 64(2),

---

33 Hijmans 2016, pp. 390-393.
34 Jay 2017, at 21-017.
35 CIPL 2016B, p. 4.
37 Council Interinstitutional File One-Stop.
38 Art. 56 (3).
The ambiguity of the applicability of the exception to the exception continues in Article 56(4). Even in cases where the lead authority decides to handle the case, the local DPA remains in a strong position. It may submit a draft decision and the lead DPA must take the utmost account of this draft. Also, this deserves attention: whereas the cooperation mechanism in enforcement cases - under Articles 56(1) and 60 GDPR – is governed by a presumption of equality of DPAs and an endeavour to reach consensus, the handling of local cases is based on a different approach. Arguably, the lead DPA is in charge of the procedure and the local DPA is in charge of the substance.

It can be questioned whether this approach by the EU legislator is practical, especially since it will often not be evident in practice which cases fall within the scope of Article 56(2). It may be for this reason that the guidance of the WP29 departs from the text of the GDPR. The Working Party underlines co-operation, with due respect for each other’s views, and describes the case of two DPAs agreeing on who is the most appropriate to take the lead in dealing with the matter, also based on input of the concerned controller or processor.39

Finally, a few observations on the scope of the exception under Article 56(2).

First, Article 56(2) applies to situations where the subject matter only relates to an establishment ‘in’ one Member State. The wording is different from the definition of cross border processing which refers to “the context of the activities” of an establishment.40 Not much is said about the meaning of this wording in Article 56(2). Recital 127 – already mentioned – uses as an example the processing of employees' personal data in the specific employment context of a Member State; the WP29 simply repeats this in its guidance.41 There is as yet no indication that the meaning of ‘subject matter’ in Article 56 (2) differs from the meaning of “the context of the activities.”

Second, Article 56(2) is applicable when the subject matter substantially affects data subjects only in one Member State. The assessment whether data subjects in other Member States are substantially affected may benefit from the WP 29’s guidance. This guidance explains that the processing must have some form of impact on the data subjects, to be examined on a case by case basis. In addition, it provides some examples of this impact, which – to a certain extent – are comparable to the examples of risk for the data subject in recital 75 GDPR. The WP29 also mentions recital 135, which – in the consistency mechanism – substantially requires ‘a significant number of data subjects in several Member States’ to be affected.42

Third, the wording of Article 56(2) is slightly different from the definition of cross border processing which also includes ‘likely to substantially affect’. It can be argued that the narrower definition of Article 56(2) means that this provision should not be applied in cases where there is doubt whether data subjects in other Member States are substantially affected. In short, when there is a possibility of risk to a significant

40 Art. 4 (23). The related provision in the DPD was interpreted in Case C-131/12, Google Spain, at paras 50-58 in a wide manner. See Gömann 2017, at 2.1.1.
41 WP29 2017, p. 5.
42 Ibid., p. 3.
number of data subjects in another Member State, Article 56(2) should not be applied on the basis of the criterion of substantial effect.

5. *Article 56 (3), (4) and (5): Procedural matters*

Article 56 paragraphs (3), (4) and (5) lay down the procedure to be respected when Article 56 (2) applies. The procedure is included in the law to ensure that the exception of Article 56(2) does not disrupt the effective handling of enforcement cases. The starting point is that the local DPA takes the initiative and the lead DPA decides whether it takes the case. This is the division of tasks laid down in Article 56(3). However, it remains to be seen if this division will be applied in practice.

One can very well imagine the situation that a lead DPA considers that a case it investigates is mainly of a local nature. In that situation, it can ask the local DPA to take the case. This would be in compliance with the GDPR, although the procedural rules in Article 56 paragraphs (3) and (4) would not be applicable. This situation would be governed by Article 56(5).

Article 56 paragraphs (3) and (4) govern the procedure starting with the initiative of the local DPA. Article 56(3) lays down a deadline for deciding on the request of the local DPA – three weeks – and includes a consideration that should be taken into account by the lead DPA. If the controller or the processor has an establishment in the country of the local DPA, it makes more sense that the local DPA takes the case, for reasons of effective enforcement.\(^{43}\) The GDPR, however, does not specify that the presence of this establishment requires the case to be taken by the local DPA and that the absence of such establishment means that the lead DPA is competent.

GDPR Article 56(4) is a remarkable provision. Even in situations where the lead DPA takes the case, the local DPA is empowered (though not required) to prepare a draft decision, in which case the lead DPA must take the utmost account of that draft.

All in all, one can argue that the legislator has a clear preference for local cases to be handled by the local DPA. However, this clear preference has not led to a clear legislative text.

6. *Article 56(6): The concept of a single interlocutor*

The lead DPA is the sole interlocutor. The term interlocutor is commonly understood as ‘a person who takes part in a dialogue or conversation’.\(^{44}\) This is also the meaning that can be deduced from other language versions of the GDPR.\(^{45}\)

This provision is part of the wider consequence of Articles 56 and 60 GDPR where normally the lead DPA is the master of the procedure. The lead DPA takes the initiative, interacts with the controller and processor (and possibly other concerned parties) and takes the decision.

---

\(^{43}\) Rec. 127.

\(^{44}\) English Oxford Living Dictionaries.

\(^{45}\) E.g. “gesprekspartner” (NL) or “Ansprechpartner” (DE). The French version uses “interlocuteur”.

*Hijmans*
The added value of Article 56 (6) may not be the notion `interlocutor` itself but rather the emphasis that this is the sole interlocutor, which suggests exclusiveness. It may very well be that this is precisely what the legislator had in mind: to preclude a controller (or processor) which operates in multiple Member States from discussing issues with multiple DPAs seeking for the best outcome. On the basis of Article 56(6), other (concerned) DPAs have an instrument to refer the controller to the lead DPA. Exclusive contacts with a controller or processor are a means to streamline the procedure.

This does not mean that the lead DPA effectively operates as the sole contact point of the lead DPA. In view of the strong position of the local DPA on substance, as described, it would be illogical to preclude the local DPA from interacting with the controller or processor. How could the local DPA prepare a draft decision, if it were not in a position to verify the facts directly with the controller or processor?

Furthermore, it is not clear whether Article 56(6) also has implications for the consistency mechanism and whether it means that the EDPB should refer a controller or processor, which is directly impacted by a case before the consistency mechanism, to its lead DPA. Would such an approach not be contrary to the right to good administration by EU bodies enshrined in Article 41 of the Charter? Article 41(2) provides the right of every person to be heard, before any individual measure which would affect him or her adversely is taken, and to have access to his or her file. It also includes an obligation of the EU administration to give reasons for its decisions. The EDPB as an EU body under Article 68(1) GDPR is part of the EU administration.

These are just two examples of a multitude of situations that may exist under the GDPR and where guidance by the EDPB might be required.

Finally, strictly speaking, the fact that a local DPA handles a case in accordance with Article 56(2) does not mean that the lead DPA is no longer the sole interlocutor, even for this case. This may be an awkward result, since Article 56(5) requires the local DPA to handle the practical conduct of the case with regard to other authorities under Articles 61 and 62, but this is what the text of Article 56 implies. A common sense approach will be required where the lead DPA recognises the practical consequences of its decision under Article 56(5) not to handle the case. Indeed, data protection authorities will have to apply common sense and goodwill generally for this part of the GDPR to work effectively.
Select Bibliography

Legislation

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 [ETS 181].


Academic writings


Hijmans, ‘The DPAs and their cooperation: how far are we in making enforcement of data protection law more European?’ 2(3) EDPL (2016), 362.


Papers of data protection authorities


Reports


Phaedra-Project, ‘Recommendations for improving practical cooperation between European Data Protection Authorities’, Deliverable D4.1, available at

Others


Article 95

Relationship with Directive 2002/58/EC

Piedade Costa de Oliveira*

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

Relevant recital

(173) This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council, including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation.

CLOSELY RELATED PROVISIONS

Article 94 (repeal of Directive 95/36/EC)

RELATED ARTICLES IN EPD [Directive 2002/58/EC]

Article 1(2) (relationship with Directive 95/46/EC) (see also recitals 10 and 12)

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 Kärntner Landesregierung, Seitlinger and Others, judgment of 8 April 2014 (ECLI:EU:C:2014:238).

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

Case C-450/06, Varec SA v Belgian State, judgment of 14 February 2008 (ECLI:EU:C:2008:91).

Case C-419/14, WebMind Licenses Kft., judgment of 17 December 2015 (ECLI:EU:C:2015:832).

ECtHR


Niemietz v Germany, judgment of 16 December 1992, Series A n° 251-B.

Peck v The United Kingdom, Appl. No. 44647/98, ECHR 2003-I.

Société Colas Est and Others v France, Appl. No 37971/97, ECHR 2002-III.


Costa de Oliveira
A. Rationale and Policy Underpinnings

Article 95 establishes the relationship between the GDPR and the ePrivacy Directive 2002/58/EC (EPD) by laying down the principle that the GDPR should not impose additional obligations with the same objective on controllers that are subject to the specific obligations laid down in the EPD. This means that regarding matters specifically governed by the EPD, including rights conferred on natural persons, the EPD should apply instead of the general rules. However, in all other cases the GDPR should apply. The basic rationale for this endeavour is to offer more legal certainty as to the provisions on the processing of personal data that are applicable in the context of the use of publicly available electronic communications services in public communication networks in the EU. This was considered necessary by the Commission (Article 89 of the proposal) and was confirmed by the EU legislator. Given the novelties introduced by the GDPR, including the range of new obligations for data controllers (and joint controllers and processors), without Article 95 it could be argued that providers of electronic communications services might need to comply also with certain obligations laid down by the GDPR, notably, because it is lex posterior.

For a correct understanding of the relationship between the GDPR and EPD, it is useful to recall that both acts have as their main purpose to implement to different degrees Articles 7 and 8 of the Charter. Indeed, the GDPR constitutes a detailed elaboration of Article 8 whereas the EPD implements Articles 7 and 8. It should be noted that the EPD is so far the only instrument in EU secondary law that comprehensively implements the principle of confidentiality of communications in Article 7 of the Charter, by laying down rules on the processing of traffic, communication and location data and the protection of terminal equipment. Vis-à-vis the GDPR it particularises data protection rules for the specific economic sector to which it applies. The EPD also ensures the confidentiality of communications of legal persons and protects their legitimate interests in this regard.

The need to protect confidentiality of communications has long been recognised. It is part of Article 8 ECHR as interpreted by the ECtHR and is in line with the constitutional traditions of EU Member States. Indeed, the majority of EU Member States recognise confidentiality of communications as a distinct constitutional right. At EU level, Directive 97/66/EC adopted in 1997 was the first specific Directive for the processing of personal data in the telecommunications sector, the predecessor of

* The views expressed are solely those of the author and do not necessarily reflect those of the European Commission.
1 See rec. 173 GDPR.
2 See most recently ECtHR, Bărbulescu v. Romania, at paras. 72-73.
4 Directive 97/66/EC.
B. Legal Antecedents

1. EU legislation

Article 95 GDPR has no equivalent in the Data Protection Directive (DPD). The relationship between the two Directives is established by Article 1(2) EPD according to which the ‘provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. […]’.

Recital 10 EPD further states that ‘in the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this directive, including the obligations on the controller and the rights of individuals. [...]’.

2. National legislation


Certain provisions of these national laws will be unaffected by the entry into application of the GDPR because of Article 95.

3. Case law

The CJEU has on several occasions ruled on the interpretation of the EPD together with the DPD. In situations which concerned the processing of personal data and privacy in the electronic communications sector, the Court focused on the relevant provisions of the EPD. Such was the case in its landmark judgments Digital Rights Ireland and Tele2 Sverige and Watson, both concerning the compatibility of data retention measures (EU and national, respectively) with the Charter.

In Digital Rights Ireland, the Court declared Directive 2006/24/EC invalid, leaving national data protection measures under the aegis of the derogation in Article 15 EPD.

In Tele2 Sverige and Watson, the Court first determined whether the national measures in question constituted implementation of EU law in the sense of Article 51(1) of the Charter. To that effect, the Court looked, in the first place, at the scope of the EPD as defined by Article 1(3) thereof, which excludes ‘activities of the State’ in specified fields, including the activities of the State in areas of criminal law and in the

\[\text{Article 95 GDPR has no equivalent in the Data Protection Directive (DPD). The relationship between the two Directives is established by Article 1(2) EPD according to which the ‘provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. […]’}.\]

\[\text{Recital 10 EPD further states that ‘in the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this directive, including the obligations on the controller and the rights of individuals. [...]’}.\]

\[\text{A list of national transposition measures communicated by the Member States concerning the EPD is available in Eur-Lex: http://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32002L0058&qid=1508243542130.}\]

\[\text{Certain provisions of these national laws will be unaffected by the entry into application of the GDPR because of Article 95.}\]

\[\text{The CJEU has on several occasions ruled on the interpretation of the EPD together with the DPD. In situations which concerned the processing of personal data and privacy in the electronic communications sector, the Court focused on the relevant provisions of the EPD. Such was the case in its landmark judgments Digital Rights Ireland and Tele2 Sverige and Watson, both concerning the compatibility of data retention measures (EU and national, respectively) with the Charter.}\]

\[\text{In Digital Rights Ireland, the Court declared Directive 2006/24/EC invalid, leaving national data protection measures under the aegis of the derogation in Article 15 EPD.}\]

\[\text{In Tele2 Sverige and Watson, the Court first determined whether the national measures in question constituted implementation of EU law in the sense of Article 51(1) of the Charter. To that effect, the Court looked, in the first place, at the scope of the EPD as defined by Article 1(3) thereof, which excludes ‘activities of the State’ in specified fields, including the activities of the State in areas of criminal law and in the}\]
areas of public security, defence and State security, including the economic well-being of the State when the activities relate to State security matters. The Court noted, however, that Article 3 EPD states that this directive is to apply to the processing of personal data in connection with the provision of ‘electronic communications services’. It further considered that, having regard to the general structure of the EPD, Article 15(1) necessarily presupposes that the national measures referred to therein, fall within the scope of that Directive. The Court therefore concluded that the Directive must be regarded as regulating the activities of the providers of such services, including those consisting in granting authorities access to the retained data.

Secondly, the Court interpreted Article 15(1) EPD in the light of Articles 7, 8, 11 and 52(1) of the Charter. It observed that, as stated in recital 2 thereof, the EPD seeks to ensure, in particular, full respect for the rights set out in Articles 7 and 8 of the Charter and that the EU legislature sought ‘to ensure that a high level of protection of personal data and privacy will continue to be guaranteed for all electronic communications services regardless of the technology used’. The Court further observed that the principle of confidentiality of communications established by the EPD implies, inter alia, that, as a general rule, any person other than the users is prohibited from storing, without the consent of the users concerned, the traffic data related to electronic communications. The only exceptions relate to persons lawfully authorised in accordance with Article 15(1) of that directive and to the technical storage necessary for conveyance of a communication.

After examining the compatibility of the national measures at issue in the light of Articles 7, 8 and 11 of the Charter, the Court concluded that national legislation such as that at issue in the main proceedings exceeds the limits of what is strictly necessary. Hence, it could not be considered to be justified, within a democratic society, as required by Article 15(1) EPD, read in the light of Articles 7, 8, 11 and 52(1) of the Charter.

C. Analysis

1. Lex generalis to lex specialis

Before analysing Article 95 GDPR, it is appropriate to explain briefly the rationale for including both natural and legal persons as beneficiaries of the rights conferred by the EPD. The main purpose of this Directive is to ensure confidentiality of communications and, to that effect, its provisions particularise and complement the general rules on the protection of personal data. The reason for including legal persons in its scope is connected with the scope of Article 7 of the Charter. This provision contains rights corresponding to those guaranteed by Article 8(1) ECHR. In accordance with Article 52(3) of the Charter, Article 7 thereof is thus to be given the same meaning and the same scope as Article 8(1) ECHR, as interpreted by the ECtHR. Concerning the scope of Article 7 as concerns legal persons, the case law of the CJEU and of the ECtHR confirms that professional activities of legal persons

---

9 Ibid., at para. 82
10 Ibid., at para. 85
11 Ibid., at para. 107
12 Case C-419/14, WebMind Licenses, at para. 70 and case-law cited therein.
13 C-450/06, Varec SA, at para. 48.
may not be excluded from the protection of the right guaranteed by both Article 7 of the Charter and Article 8 of the Convention.\textsuperscript{14}

As the EPD specifically governs the processing of personal data by providers of electronic communications services falling within its scope, it must be regarded as a \textit{lex specialis},\textsuperscript{15} as is explicit in Article 1(2) thereof.

Article 95 GDPR was part of the Commission’s proposal of 2012.\textsuperscript{16} The then Article 89 of the proposal contained two paragraphs: paragraph 1, which corresponds to Article 95, and a second paragraph intended to amend the EPD by deleting its Article 1(2). The amendment to the EPD was not retained by co-legislators.\textsuperscript{17} The result is that the relationship between the EPD and the GDPR is therefore established in both acts. Indeed, given that any references to Directive 95/46/EC must be construed as references to the GDPR (see Article 94(2) GDPR), arguably Article 95 was not necessary. In the author’s view, it is nevertheless a useful clarification as to the obligations that are applicable to communications service providers, notably during the period pending the adoption of the proposed ePrivacy Regulation.

Regarding the matters for which controllers are subject to ‘specific obligations with the same objective,’ as referred to in Article 95, an example is Article 4 EPD on security of processing. Article 4(1) requires communications service providers to take appropriate technical and organisational measures to safeguard the security of their services, and thus departs from the objective of protecting personal data. However, Article 4(1a), introduced by Directive 2009/136/EC, obliges communications service providers to put in place a number of mandatory measures aiming specifically at ensuring the protection of personal data (access limited to authorised personnel for legally authorised purposes; protection against accidental or unlawful destruction, accidental loss or alteration; implementation of a security policy with respect to processing). Furthermore, Article 4(3) imposes on the same providers the obligation to notify the competent authority (and in certain circumstances, the person concerned) of a personal data breach, falling within the same objective as the GDPR. This means that communications service providers will not be requested to comply with the provisions of Articles 32 to 34 GDPR.\textsuperscript{18} Article 95 is thus the logical consequence of a specific regime that is not modified by the GDPR and which regulates the core aspects of the processing of personal data (grounds for processing, purposes, retention periods, security measures, personal data breach notifications) in connection with the provision and use of electronic communications in publicly available communications services and networks.\textsuperscript{19}

\textsuperscript{15} This is also explicit in rec. 173: it states that the GDPR applies to all matters concerning the processing of personal data which are not subject to specific obligations with the same objective set out in the EPD, including the obligations on the controller and the rights of natural persons.
\textsuperscript{16} GDPR Proposal.
\textsuperscript{17} Rec. 173 GDPR still makes reference to the amendment of that Directive (as proposed in rec. 135).
\textsuperscript{18} Art. 32 on security of processing builds on Art. 17 DPD and Art. 33 and Art. 34 on data breach notifications build on Art. 4(3) EPD. Also, the definition of personal data breach under Art. 4(12) GDPR is based on Art. 2(i) EPD as amended by Directive 2009/136/EC.
\textsuperscript{19} It is interesting to note that Art. 95 GDPR was adopted almost without modifications as compared to Art. 89 of the Commission’s proposal with the sole difference that the Commission proposed to amend
2. The proposal for the ePrivacy Regulation (EPR)

Recital 173 states that once the GDPR is adopted, the EPD should be reviewed, in particular to ensure consistency with this Regulation. In reply to this call by the co-legislators, the Commission adopted the proposal for the EPR on 10 January 2017.\textsuperscript{20} The text of Article 1(3) of that proposal is similar to current Article 1(2) EPD and provides that the provisions of the EPR \textit{particularise and complement} the GDPR \textit{by laying down specific rules} […] This means that all matters concerning the processing of personal data not specifically addressed by the proposal are covered by the GDPR. As the adoption of the EPR will take place some time after 25 May 2018 (when the provisions of the GDPR start to apply), there will be a period where the GDPR and the EPD overlap, as contemplated by Article 95.

The Commission’s choice of the instrument (a Regulation) for electronic communications privacy follows the same rationale as for the GDPR: to ensure legal certainty for users and businesses alike by avoiding divergent interpretation and implementation in the Member States. It is also justified for reasons of consistency with the GDPR.

The proposal contains a set of targeted measures aimed at ensuring effective protection of the fundamental right to privacy and communications. To that effect, it lays down the principle of confidentiality of communications and identifies exhaustively the permitted processing of communications data. It enlarges the personal scope of the current EPD to extend to Over-the-Top communications services (OTTs).\textsuperscript{21} This takes into account the reality that users increasingly replace traditional voice telephony, text messages (SMS) and electronic mail conveyance services in favour of functionally equivalent online services such as Voice over IP, messaging services and web-based e-mail services.

The proposal also extends the principle of confidentiality of communications to the transmission of machine-to-machine communications and reinforces the protection of privacy of terminal equipment.\textsuperscript{22} The alignment with the GDPR resulted in incorporating its definitions, territorial scope and the supervision and consistency mechanism into the EPR. It also resulted in the omission in the proposal of some

\begin{thebibliography}{9}
\bibitem{173} Recital 173 GDPR still makes reference to the amendment of that Directive (as proposed in rec. 135).
\bibitem{20} EPR Proposal.
\bibitem{21} The EPD is part of the regulatory framework for electronic communications. This framework was revised in 2016 following which the Commission adopted the EECC Proposal. The proposal for EPR, partially relies on definitions provided in the EECC Proposal, including that of 'electronic communications services'. Like the EECC Proposal, the EPR Proposal also brings OTT providers in its scope to reflect the market reality.
\bibitem{22} The Explanatory Memorandum accompanying the EPR Proposal states that ‘the consent rule to protect the confidentiality of terminal equipment failed to reach its objectives as end-users face requests to accept tracking cookies without understanding their meaning and, in some cases, are even exposed to cookies being set without their consent. The consent rule is over-inclusive, as it also covers non-privacy intrusive practices, and under-inclusive, as it does not clearly cover some tracking techniques (e.g. device fingerprinting) which may not entail access/storage in the device. Finally, its implementation can be costly for businesses'.
\end{thebibliography}
provisions, such as the security and data breach notification obligations of Article 4 EPD, to ensure that those provisions already in the GDPR will apply. Finally, as some of the rules in the EPD apply also to legal persons, certain provisions of the GDPR will be applicable to this category of end-users, notably those on consent and on legal remedies and compensation, as provided for under Articles 77, 78, 79 and 82 GDPR.
Select Bibliography

Legislation


Papers of data protection authorities
