Principles relating to processing of personal data

De Terwangne, Cecile

Published in:
The EU general data protection (GDPR)

Publication date:
2020

Document Version
Publisher's PDF, also known as Version of record

Chapter II Principles (Articles 5–11)

Article 5. Principles relating to processing of personal data

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.

Closely Related Provisions

Article 6(1) (Lawfulness of processing) (see too recitals 40–49); 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 58–59); Articles 13–15 (Information and access to personal data) (see also recitals 60–64); Article 24 (Responsibility of the controller) (see too recitals 74–78) ; 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 158–163)

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

Article 4 (Principles relating to processing of personal data) (see too recitals 26–28); Article 9(1) and (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)

Related Provisions in EUDPR [Regulation (EU) 2018/1725]

Article 4 (Principles relating to processing of personal data) (see too recitals 20–22); Article 5(1) (Lawfulness of processing) (see also recitals 22–24); Article 6 (Processing for another compatible purpose) (see too recital 25); Article 14 (Transparent information) (see too recitals 34–36); Articles 15–17 (Information and access to personal data) (see also recitals 35–37); Article 26 (Responsibility of the controller) (see too recitals 45–48) ; Article 33 (Security of processing) (see too recitals 53–54); Article 71 (Principles relating to processing of operational personal data); Article 72 (Lawfulness of processing operational personal data); Articles 78–83 (Information and access with respect to operational personal data); Article 91 (Security of processing of operational personal data)

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 (Grand Chamber) (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 and Others*, judgment of 8 April 2014 (Grand Chamber) (ECLI:EU:C:2014:238).
Case C-683/13, *Pharmacontinente – Saude e Higiene SA*, order of 19 June 2014 (ECLI:EU:C:2014:2028).
Case C-201/14, *Smaranda Bara and Others v Casa Națională de Asigurări de Sănătate and Others*, 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 (Grand Chamber) (ECLI:EU:C:2016:970).
Case C-708/18, *TK v Asociația de Proprietari bloc M5A Scara-A* (pending).

ECtHR

Gaskin v United Kingdom, Appl. No. 10454/83, judgment of 7 July 1989.
M.S. v Sweden, Appl. No. 20837/92, judgment of 27 August 1997.
Rotaru v Romania [GC], Appl. No. 28341/95, judgment of 4 May 2000.
Copland v United Kingdom, Appl. No. 62617/00, judgment of 3 April 2007.
S. and Marper v United Kingdom, Appl. No. 30562/04, 30566/04, judgment of 4 December 2008.
Haralambie v Romania, Appl. No. 21737, judgment of 27 October 2009.
K.H. and Others v Slovakia, Appl. No. 32881/04, judgment of 28 April 2009.
Szabo and Vissy v Hungary, Appl. No. 37138/14, judgment of 12 January 2016.

A. Rationale and Policy Underpinnings

Article 5 GDPR lays down all the key principles providing the basis for 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 (Article 5(1)(a)) which takes the form of a duty to inform data subjects (Articles 12 and following), as well as for the integrity and confidentiality principle (Article 5(1)(f) which is elaborated in Articles 32 and following), and for the accountability principle (Article 5(2)) which is elaborated in, inter alia, Articles 24 and 25).

Data protection fundamental principles have not been substantially modified compared with the other rules governing this field for several decades. The principles laid down in the 1980 OECD Guidelines[1] and in the Convention 108 of 1981 have demonstrated their capacity to stand the test of time: 'More than 30 years of practical application have proven these principles to be sound'.[2] 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 95/46—and in Article 5 of the Convention 108—must be amended'.[3] In consequence, the GDPR does not make fundamental changes to these principles. Nonetheless, certain adjustments and additions have been made in the GDPR, as shown in the following commentary.

[1] OECD Guidelines 2013.
[2] Kotschy 2016, p. 277. See also de Terwangne 2014.
[3] Kotschy 2016, p. 277.

B. Legal Background

1. EU legislation

Article 6(1) DPD contained virtually the same principles as Article 5 GDPR. It was entitled 'Principles relating to data quality', although it dealt with more than just data quality. It set out principles relating to the lawfulness and fairness of processing; purpose limitation; data minimisation; the accuracy of data; and storage limitation. All these principles were formulated very similarly to the GDPR. Contrary to Article 5 GDPR, Article 6 DPD omitted mention of the principle of integrity and confidentiality, which is arguably logical since this provision was dedicated to data quality—even if certain principles contained therein went beyond the mere matter of data quality. In contrast, Article 5 GDPR is entitled 'Principles relating to processing of personal data' and has a wider scope. Provisions on the integrity and confidentiality of processing were found in Articles 16 and 17 DPD. No accountability principle was stated as such but Article 6(2) DPD clarified all the same that '[i]t shall be for the controller to ensure that paragraph 1 is complied with'.

Article 4 EUDPR contains provisions that are essentially identical to those of Article 5 GDPR, and the former should be interpreted in the same way as the latter (see too recital 5 EUDPR). In contrast, the equivalent principles set out in Article 4 LED, while largely similar to their GDPR and EUDPR counterparts, contain some differences (highlighted in the analysis below), so that care must be taken when applying to them a line of interpretation derived from the GDPR or EUDPR.

2. International instruments

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 replicated its provisions while 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 entitled 'Data security' requires appropriate security measures to be taken for the protection of personal data 'against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination'. There is, however, no specific trace of the accountability principle in the Convention.

The Modernised Convention 108 brings new elements in relation to 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 disclosure of personal data' (Article 7(1)). It is supplemented by a new data breach notification duty (Article 7(2)). The accountability principle appears in the new Article 10(1) which states that parties shall provide that controllers and processors must take all appropriate measures to comply with the obligations of the Convention as originally adopted 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*[5] that 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 legitimate purpose). The Court has examined the respect for this principle of proportionality 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 retention. The Court went even further in the *Tele2* case,[7] where it stated that legislation prescribing a general and indiscriminate retention of personal data exceeds the limits of what is strictly necessary and cannot be considered as justified. Proportionality considerations also come to the fore in the recent *TK* case[8] where the Court has been asked to assess, inter alia, whether video surveillance is excessive or inappropriate with respect to Article 6(1)(e) DPD where the controller is able to take other measures to protect the legitimate interest in question.

The ECtHR has repeatedly ruled that processing of personal data may in particular circumstances constitute an interference with the data subject's right to respect for private life under Article 8(1) of the European Convention on Human Rights ('ECHR').[9] To be justified, such an interference must, inter alia, be in accordance with the law (Article 8(2) ECHR), which can be correlated with the requirement for lawful processing. This law must be foreseeable as to its effects. In the *Rotaru* case,[10] the Court indicated that, to be foreseeable, 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 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, email and internet usage, without the data 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(1) ECHR.[11] The Court has also stated that data subjects have a qualified right of access to their data.[12] 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.[13]

In the *S. and Marper* case,[14] the Court affirmed that data processing which interferes with rights under Article 8(1) ECHR must be proportionate, that is to say appropriate in

[4] Case C-201/14, *Bara*, paras. 34 et seq.
[5] Joined Cases C-92/09 and 93/09, *Schecke*, paras. 86–89.
[6] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*.
[7] Joined Cases C-203/15 and C-698/15, *Tele2*, para. 107.
[8] Case C-708/18, *TK*.
[9] See generally Bygrave 2014, pp. 86 ff.
[10] ECtHR, *Rotaru v Romania*.
[11] ECtHR, *Copland v UK*.
[12] See e.g. ECtHR, *Haralambie v Romania*; ECtHR, *Gaskin v UK*.
[13] ECtHR, *M.S. v Sweden*, para. 35.
[14] ECtHR, *S. and Marper v UK*.

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, the processing should not lead to a disproportionate interference with these individual or collective interests in relation to the benefits expected from the controller. In particular, the retention of the data must be proportionate in relation to the purpose of collection and must be limited in time.[15] As stated by the Court in *S. and Marper*: 'The domestic law should ... 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'.[16]

C. Analysis

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

The first basic principle 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, the requirement that data processing must be *lawful* essentially means 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 core conditions for processing to be lawful. In fact, Article 6(1) GDPR states that processing shall be lawful only if and to the extent that at least one of the conditions it lists applies.[17] In the same way, 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,[18] 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 Charter of Fundamental Rights of the European Union ('CFR') 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 that 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.[19] 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 before the GDPR commentators had read the transparency requirement into the notion of fairness.[20]

The *transparency* principle is explained in 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 end, 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 concerning the quality and content of this information duty are the subject of Articles 12–14 dedicated to 'Transparency and modalities'.[21] Certain aspects 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 crime prevention activity or of the criminal investigation of public authorities. However, fairness of processing is still required and may imply a certain dose of transparency.[22]

2. Purpose limitation principle—Article 5(1)(b)

The purpose limitation principle has long been regarded as a 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)[23] and not further processed in a manner that is incompatible with those purposes (the 'compatible use' dimension).[24] 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.[25] 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:[26]

> 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.[27]

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 limitation 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 mark it out better. Thus,

[15] See also ECtHR, *Szabo and Vissy v Hungary*.
[16] ECtHR, *S. and Marper v UK*, para. 103.
[17] See further the commentary on Art. 6 in this volume.
[18] FRA 2014, pp. 64 et seq.
[19] See for a case of unfair processing: ECtHR, *K.H. and Others v Slovakia*.
[20] See e.g. FRA 2014, p. 76 ('Fair processing means transparency of processing, especially vis-à-vis data subjects'); Bygrave 2014, p. 147.
[21] See further the commentaries on Arts. 12 to 14 in this volume.
[22] See also Art. 13 LED ('Information to be made available or given to the data subject') and Art. 14 LED ('Right of access by the data subject').
[23] WP29 2013, pp. 11 and 12.
[24] Ibid., pp. 12 and 13.
[25] Ibid., p. 39.
[26] Boulanger et al. 1997.
[27] Explanatory Report Convention 108 2018, p.8.

Article 6(4) offers a series of criteria 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.[28] 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.[29]

Another new element of the GDPR is the clarification that processing personal data for a purpose other than that for which they have been collected is allowed in certain circumstances even if this new purpose is not compatible with the first one. Indeed, the original Commission Proposal for the GDPR opened up this possibility very widely, which would have reduced the purpose limitation principle to the bare bones. The Council initially wanted to go even further by proposing to authorise further processing for incompatible purposes if done by the same controller and provided that the controller's or a third party's legitimate interests prevailed over the data subject's interests.[30] This proposal, which was heavily criticised,[31] would have rendered the purpose limitation principle void and truly meaningless. The final text has come back to the protective aim of the purpose limitation 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.[32] 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 reuses of data are a priori considered as compatible provided certain conditions are met,[33] 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'.[34] 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'. Some elucidation 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.[35] The category of data processing for statistical purposes has remained unchanged.[36] 'Statistical purpose'

[28] This list is based on the one elaborated by the WP29: see WP29 2013, p. 40.
[29] Art. 6(4) GDPR. See also rec. 50 GDPR.
[30] This proposal was aimed at facilitating 'Big Data' operations: see Burton et al. 2016, p. 6.
[31] See notably WP29 Press Release 2015 and WP29 2013, pp. 36 and 37.
[32] See the commentary on Art. 6 in this volume.
[33] These conditions are developed in Art. 89(1) GDPR.
[34] Ibid., Art. 5(1)(b).
[35] Explanatory Report Convention 108 2018, p. 3.
[36] See the detailed regime for processing for statistical purposes in COM Recommendation 1997.

refers to the elaboration of statistical surveys or the production of statistical, aggregated results.[37] Statistics aim at analysing and characterising mass or collective phenomena in a considered population.[38]

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.[39] Article 4(3) LED states that processing falling within 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.

3. Data minimisation principle—Article 5(1)(c)

As was the case 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. However, under the GDPR personal data must be 'limited to what is necessary' instead of being 'not excessive' as in the DPD. The LED, though, has kept the wording of the DPD; thus, Article 4(1)(c) LED states that data must be 'not excessive'. This difference of terms should not have a substantial effect on the scope of the data minimisation principle. Recital 39 GDPR 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 accordingly clear that one may not process an excessively large amount of personal data (asking an employee for her complete medical file to assess her 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).[40] 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 them. 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

[37] Ibid., Appendix, point 1.
[38] Explanatory Report Convention 108 2018, p. 9.
[39] Council Framework Decision 2008/977/JAI.
[40] See Explanatory Report Convention 108 2018, p. 9, for an explanation of the notion of 'excessive' data.

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 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 of the GDPR dedicated to controllers and processors develops this duty of security.[41] 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 29–31).

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 (accountability).[42] This requirement not only to ensure but also to be able to demonstrate compliance to

[41] See the commentary on Arts. 32–34 in this volume.

[42] WP29 2010.

GDPR is developed in Article 24 dedicated to the responsibility of the controller.[43] Much important work on accountability has also been done by think-tanks such as the Information Accountability Foundation.[44]

Select Bibliography

International agreements

OECD Guidelines 2013: Organisation for Economic Co-operation and Development, 'The OECD Privacy Framework' (2013).

EU legislation

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ 2008 L 350/60.

Academic writings

Boulanger et al. 1997: Boulanger, de Terwangne, Léonard, Louveaux, Moreaux and Poullet, 'La Protection des données à caractère personnel en droit communautaire', *Journal des tribunaux—Droit Européen* (1997), 145.

Burton et al. 2016: Burton, De Boel, Kuner, Pateraki, Cadiot and Hoffman, 'The Final European Union General Data Protection Regulation', *Bloomberg Law: Privacy & Data Security* (12 February 2016).

Bygrave 2014: Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014).

De Terwangne 2014: 'The Revision of the Council of Europe Convention 108 for the Protection of Individuals as Regards the Automatic Processing of Personal Data', 28 *International Review of Law, Computers & Technology* (special edition *The Future of Data Protection: Collapse or Revival?*) (2014), 118.

Kotschy 2014: Kotschy, 'The Proposal for a new General Data Protection Regulation—Problems Solved?', 4(4) *International Data Privacy Law* (2014), 274.

Papers of data protection authorities

WP29 2010: Article 29 Working Party, 'Opinion 3/2010 on the Principle of Accountability' (WP 173, 13 July 2010).

WP29 2013: Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation' (WP 203, 2 April 2013).

WP29 Press Release 2015: Article 29 Working Party, 'Press Release on Chapter II of the Draft Regulation for the March JHA Council' (17 March 2015).

Reports and recommendations

COM Recommendation 1997: Committee of Ministers of the Council of Europe, 'Recommendation Concerning the Protection of Personal Data Collected and Processed for Statistical Purposes' (Rec(1997)18, 30 September 1997).

De Terwangne and Moiny, 'The Lacunae of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) Resulting from Technological

[43] See further the commentary on Art. 24 in this volume.

[44] See Information Accountability Foundation website.

Developments' (2010), available at http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2010_09_en.pdf.

Explanatory Report Convention 108 2018: Council of Europe, 'Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data' (10 October 2018), available at https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.

FRA 2014: European Union Agency for Fundamental Rights, European Court of Human Rights, Council of Europe, and European Data Protection Supervisor (eds.), *Handbook on European Data Protection Law* (Publications Office of the European Union 2014).

Others

Information Accountability Foundation Website: Information Accountability Foundation, available at https://informationaccountability.org.