United Nations A/77/196

General Assembly

Distr.: General
20 July 2022
English
Original: Spanish

Seventy-seventh session
Item 69 (b) of the provisional agenda
Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms

Right to privacy

Note by the Secretary-General

The Secretary-General has the honour to transmit to the General Assembly the report prepared by the Special Rapporteur on the right to privacy, Ana Brian Nougrères, submitted in accordance with Human Rights Council resolution 28/16.

22-11362 (E) 090822 170822

Summary

The principles underpinning privacy and the protection of personal data are a structural part of the legal systems relating to those issues, as they fulfil the dual function of interpreting and integrating the regulatory framework. They are the most valuable and useful means of enabling data controllers and processors to properly process personal information, particularly in the face of the risk of misuse of information and communications technologies.

The present report contains an analysis of the principles of legality, lawfulness and legitimacy, consent, transparency, purpose, fairness, proportionality, minimization, quality, responsibility and security, as these principles are the cornerstones of the entire legal system relating to privacy and the protection of personal data. The report includes a comparative study of the formulation of these principles in seven international regulatory documents, as set out below. It also highlights their common aspects, in order to work towards harmonization at the global level and address the challenge of protection of privacy and personal data as a fundamental human right that, owing to its cross-cutting nature, enables the protection of other fundamental human rights, such as the rights to freedom, equality, honour and dignity in the digital era.

Principles underpinning privacy and the protection of personal data

I. Introduction

1. There are guiding principles relating to privacy and data protection that constitute guidelines for interpretation, help to fill gaps in the law and are essential for determining ways of addressing the problems that arise when processing personal data using information and communications technologies.

2. National and international regulations in this area are general in nature. They must therefore be given concrete form in various personal data processing activities by controllers and processors operating in various sectors, whether public or private, at the national or international level, and whatever the technology[1] used. A key objective is the effective enforcement of relevant regulations, as, in a democratic system of government, mere recognition of and the development of laws concerning fundamental rights is not enough. These enshrined rights must be accompanied by effective guarantees of protection, whatever the context.

3. The guiding principles that will be analysed in the present report are therefore the most valuable and useful means of ensuring the proper processing of personal information.

4. The principles underpinning privacy and the protection of personal data should not be considered mere recommendations, as they have a higher status than recommendations. Because of that status, they are a structural part of the legal systems relating to those issues. These principles require controllers and processors to act appropriately in processing personal data and to address the risk of misuse of information and communications technologies, artificial intelligence and other technological developments, thereby enabling data subjects to retain control over their personal information.

5. These principles are closely interrelated. They must therefore be examined not only individually but as part of the set to which they belong, with a view to ensuring the proper management of personal information, while upholding relevant rights and fundamental freedoms.

6. Special categories of personal data, in particular sensitive data, should be taken into account. There is currently a consensus that such data should be subject to processing restrictions, as they require greater protection, given that they involve the most private sphere of a person's life. As a result, their processing could pose a greater risk to rights and fundamental freedoms.

7. In accordance with international regulatory documents, in most countries, sensitive data, as a general rule, should not be processed, except in cases specifically allowed under the law. This rule exists in order to eliminate the risk of discrimination against data subjects.

8. It is considered advisable for laws to indicate the categories of sensitive personal data, and to establish the scope of and exceptions to their protection. It is also legitimate for States to take into account the cultural, social and political context and local realities when determining which data belong to these categories.

[1] "Technological neutrality is of particular importance in view of speed of technological innovation and helps to ensure that legislation remains capable of accommodating future developments and does not become obsolete too quickly." United Nations Commission on International Trade Law, *Building confidence in electronic commerce: legal issues in the international use of electronic authentication and signature methods* (Vienna, 2009).

9. The processing of sensitive personal data should be allowed when their protection is appropriately guaranteed under the law. Such guarantees must specifically include the need to uphold the guiding principles relating to privacy and data protection.

10. In order to begin to develop the principles of privacy and protection of personal data at the global level, the present report contains an analysis of the guiding principles set out in seven relevant international regulatory documents.

11. The report highlights the basic common aspects, as well as some specific characteristics, of these documents, with the aim of seeking consensus to enable the harmonization of efforts to properly process personal data, while upholding the right to the protection of such data, to privacy and to dignity in the digital era.

II. Regulatory analysis

12. An analysis of the principles of legality, lawfulness and legitimacy, consent, transparency, purpose, fairness, proportionality, minimization, quality, responsibility and security is provided in the sections below. This analysis is based on the following documents:

- General Data Protection Regulation of the European Union (General Regulation)[2]
- Modernized Convention of the Council of Europe for the Protection of Individuals with Regard to the Processing of Personal Data (modernized Convention 108)[3]
- General Assembly resolution 45/95, entitled "Guidelines for the regulation of computerized personal data files" (United Nations Guidelines)
- Standards for Personal Data Protection for Ibero-American States, adopted by the Ibero-American Data Protection Network[4] (Ibero-American Standards)
- Recommendations of the Council concerning the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of the Organisation for Economic Co-operation and Development (OECD Guidelines)[5]
- Asia-Pacific Economic Cooperation (APEC) Privacy Framework (APEC Privacy Framework)[6]
- Updated Principles of the Inter-American Juridical Committee on Privacy and Personal Data Protection, with annotations, adopted by the General Assembly of the Organization of American States (OAS) (OAS Principles)[7]

Principle of legality, lawfulness and legitimacy

13. In accordance with this principle, the processing of personal data, throughout their life cycle, must be carried out by the responsible party in compliance with relevant laws and with respect for internationally recognized human rights. This means that, through the appropriate, and thus legal, processing of personal data, respect for privacy and other rights, as well as the dignity of the data subject, will be ensured.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
[3] Available at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.
[4] Ibero-American Data Protection Network, "Standards for Personal Data Protection for Ibero-American States". Available at: www.argentina.gob.ar/sites/default/files/estandares_eng.pdf.
[5] Available at: www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#recommendation.
[6] Available at: https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015).
[7] Report of the Inter-American Juridical Committee, "Updated Principles of the Inter-American Juridical Committee on Privacy and Personal Data Protection, with annotations", 9 April 2021.

14. Upholding the right to the protection of personal data, which is recognized as a right that enables the protection of other rights,[8] will ensure that the proper processing of data concerning an individual will, in turn, guarantee respect for his or her other fundamental rights.

15. Although legality must be the foundation for all processing activities throughout the life cycle of personal data, from their collection to their deletion, emphasis is usually placed on the first processing activity, namely, data collection, because if this activity is performed illegally, it will affect the legality of the other processing activities that arise from it.[9]

16. In modernized Convention 108, it is stated that data processing must pursue a legitimate purpose at all stages, and must be carried out in accordance with the law (art. 5.1).

17. Under the United Nations Guidelines, in accordance with the principle of lawfulness and fairness, personal information must be collected and processed in lawful and fair ways.

18. The various international regulatory documents have been expanding and incorporating other data protection principles that are related to and complement the principle of legality.

19. In that regard, article 6 and recitals 39 and 40 of the General Regulation provide that processing is lawful when carried out in accordance with a legal basis established by law.

20. Under the Ibero-American Standards, in accordance with the principle of legitimacy, personal data may only be processed under the conditions established by law (art. 11).

21. In line with the OECD Guidelines, data must be collected by lawful and fair means, and with the knowledge or consent of the data subject (art. 7).

22. The legality of the processing of personal data is based on the existence of legitimate grounds, as established in the applicable regulations. Table 1, setting out the internationally recognized legitimate grounds, was developed from an analysis of the relevant international regulatory documents.

[8] Article 1 of modernized Convention 108.

[9] Paragraph 7 of the OECD Guidelines; First Principle of the OAS Principles; article 1 of the Guidelines.

Table 1
Legitimate grounds for processing

	Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data	*United Nations Guidelines for the regulation of computerized personal data files*	*Standards for Personal Data Protection of the Ibero-American Data Protection Network*	*General Data Protection Regulation of the European Union*	*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*	*APEC Privacy Framework*	*OAS Updated Principles on Privacy and Personal Data Protection, with annotations*
	Article	*Article*	*Article*	*Article*	*Paragraph*	*Principle*	*Principle*
Consent of the subject	5.2		11.1 (a)	6.1 (a)	10 (a)	III.24	First
Consent of the subject for a purpose that is incompatible with that for which the data were collected		3 (b)					
Law	5.3		14.1		10 (b)	IV.25 (c)	First
Legal obligation of the controller			11.1 (f)	6.1 (c)			First
Fulfilment of a contract or precontractual steps			11.1 (e)	6.1 (b)		IV.25 (b)	First
Public interest			11.1 (h)	6.1 (e)			First
Legitimate interest of the controller			11.1 (i)	6.1 (f)			First
Vital interests of the subject or a third party			11.1 (g)	6.1 (d)			First
Recognition or defence of the subject's rights before a public authority			11.1 (d)				First
Court order, decision or mandate from a public authority			11.1 (b)				First

23. The permissible grounds for the processing of personal data are indicated below, in order of the frequency with which references to such grounds recur in the international regulatory documents analysed.

24. Six documents include the consent of the subject as one of the legitimate grounds for the processing of personal data, making it the most frequently mentioned grounds in the regulations analysed.

25. Under the United Nations Guidelines, consent is not established as a general permissible grounds, but rather as grounds for carrying out processing activities for purposes other than those for which the data were collected. Taking into account this point and article 1 of the United Nations Guidelines, in which the principle under consideration is addressed, personal data must be processed in fair and lawful ways, in accordance with the purposes of the Charter of the United Nations. This involves ensuring that a certain amount of publicity is given and that the data subject is informed.

26. The consent of the subject is followed by the authority of law or the domestic laws of each member country, grounds mentioned in five of the documents.

27. Four documents include as legitimate grounds the fulfilment of a contract or precontractual steps. The recognition of such grounds as they pertain to social and commercial relations, as well as electronic commerce, is particularly important in the economic context of the digital age.

28. Three documents recognize as legitimate grounds the legal obligation of the controller, the public interest, the legitimate interest of the controller and the vital

interests of the subject or a third party, and two documents include as legitimate grounds the recognition or defence of the subject's rights before a public authority, and a court order, decision or mandate from a public authority.

29. In order to uphold the right to the protection of personal data, privacy and dignity, irrespective of the regulatory context, one of the relevant permissible grounds must be met for a data controller and, where applicable, a processor to be able to manage personal data.

Principle of consent

30. Consent is an express or tacit demonstration of will by which the consenting party is legally bound. When data subjects give consent, their power of control over their personal data, as the subjects of such data, is directly revealed.

31. The principle of consent is closely linked to the principle of legality, as it is the most common internationally recognized permissible grounds for the processing of personal data.

32. In accordance with the principle of consent, data subjects must indicate that they accept that their personal data may be collected, recorded, processed, communicated or transferred, and, in general, that such data may be subject to any processing activity, including deletion, thereby granting controllers the power to determine the data's entire life cycle.[10]

33. In the normative documents analysed, consent is one of the most important legitimate grounds for the processing of personal data, as it is specifically identified as such in six of those documents,[11] with various characteristics.

34. The aspects mentioned below are a means of defining the parameters within which consent can be given, in order to reflect the data subject's will as faithfully as possible.

35. In table 2 below, the characteristics mentioned in the seven relevant international regulatory documents are compared.

Table 2
Characteristics of consent

	Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data	*United Nations Guidelines for the regulation of computerized personal data files*	*Standards for Personal Data Protection of the Ibero-American Data Protection Network*	*General Data Protection Regulation of the European Union*	*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*	*APEC Privacy Framework*	*OAS Updated Principles on Privacy and Personal Data Protection, with annotations*
	Article(s)	*Article(s)*	*Article(s)*	*Article(s)*	*Paragraph*	*Principle*	*Principle*
Free	5.2			4.11			Second
Specific	5.2		12	4.11			Second
Informed	5.2			7.3 and 4.11	Point 52 of the Memorandum		Second
Unequivocal	5.2		12	4.11			Second
Revocable			12.2	7.3			Second

[10] Recital 32 of the General Regulation.

[11] As stated in the earlier section on the principle of legality, lawfulness and legitimacy, in the United Nations Guidelines, consent is established only as a legitimate grounds for carrying out processing activities for purposes other than those for which the data were collected.

36. As shown, among the texts under consideration, modernized Convention 108 (art. 5.2), the General Regulation,[12] and the OAS Principles (Second Principle) attribute the highest number of characteristics to the type of consent required to protect personal data, in order to ensure that the data subject's will is faithfully reflected.

37. This type of consent, from an analysis of the characteristics mentioned in the texts, must be free, specific, informed, unequivocal and revocable. Although revocability appears to be missing from modernized Convention 108 and from the United Nations Guidelines (art. 4), the OECD Guidelines and the APEC Privacy Framework (arts. 21 to 23 and 26), it can be found in those texts, in the sections relating to the rights of data subjects.[13] Revocation is presented in those texts as a correlate of the power to consent having the opposite effect to and taking place later than the granting of consent.

38. In the case of the OECD Guidelines, the concept of informed consent does not arise in principle from the wording of the articles, in which it is stated that data must be collected, where applicable, with the knowledge or consent of the data subject. However, in the Explanatory Memorandum to the OECD Guidelines, it is stated that, while the consent of the subject may or may not be required, knowledge is the minimum requirement.[14] Therefore, when consent is required for the collection of personal data, it must be informed, as the knowledge of the data subject is the minimum requirement that must be met.

39. The characteristics of the expression of will whereby the processing of data is authorized do not always appear in articles relating to the principle of consent. However, in some of the documents, such as the General Regulation (art. 4), some such characteristics are set out in definitions and recitals.

40. Characteristics of consent are not established in the United Nations Guidelines and the APEC Privacy Framework.

41. As the permissible grounds for the processing of personal data, consent must be granted before the start of the activities for which it is being granted.

42. The principle of consent is directly linked to the principle of transparency, insofar as valid consent by a data subject implies that he or she is appropriately informed of the conditions to which his or her personal information will be subject.

43. It is important to mention the way in which consent for the processing of the personal data of minors is reflected in the documents. With regard to the protection of personal data, children and adolescents are considered to be a vulnerable group that is particularly susceptible to the consequences of the processing of information concerning them. It is therefore necessary to ensure their comprehensive protection and well-being.

44. In the Ibero-American Standards (art. 13), the General Regulation (art. 8) and the OAS Principles (Second Principle), it is indicated that the consent of minors is subject to the authorization of the holders of parental authority or of their legal representatives, as they are responsible for the consequences of the processing. These documents also provide that the domestic law of each State may establish a minimum age at which minors may give consent directly, with due safeguards.

[12] Articles 4.11; 6.3 (a) and (b); 6.1 (a), (b), (c), (d) and (e); 7; and 8.

[13] Article 9 of modernized Convention 108; article 4 of the United Nations Guidelines.

[14] Explanatory Memorandum (point 52), p. 19.

Principle of transparency

45. One of the principles relating to the processing of personal data is that controllers must process data transparently in relation to data subjects. In accordance with this principle, controllers must inform subjects of the processing conditions to which their personal information will be subject from the time of collection, so that subjects are in a position to exercise due control over the data.

46. Table 3 below shows the information that controllers must provide to data subjects, as indicated in the international regulatory documents analysed.

Table 3
Information that must be provided to data subjects

	Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data	*United Nations Guidelines for the regulation of computerized personal data files*	*Standards for Personal Data Protection of the Ibero-American Data Protection Network*	*General Data Protection Regulation*		*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*	*APEC Privacy Framework*	*OAS Updated Principles on Privacy and Personal Data Protection, with annotations*
				When the data are obtained from the subject	*When the data are not obtained from the subject*			
	Article(s)	*Article(s)*	*Article(s)*	*Article(s)*		*Paragraph*	*Principle*	*Principle*
Identity and address of the controller and/or representative	8.1 (a)		16.2 (a)	13.1 (a)	14.1 (a)	12	21 (d)	Second
Existence and/or main characteristics of the processing			16.1			12	21 (a)	
Legal foundation or basis	8.1 (b)			13.1 (c)	14.1 (c) and 14.2 (b)			Second
Aims or purpose of the processing	8.1 (b)		16.2 (b)	13.1 (c)	14.1 (c)	12	21 (b)	Second
Categories of data processed	8.1 (c)				14.1 (d)			
Origin of the data when not obtained directly from the subject			16.2 (e)		14.2 (f)			
Recipients or category of recipients	8.1 (d)		16.2 (c)	13.1 (e)	14.1 (e)		21 (c)	Second
Information on rights and the ways in which to exercise them	8.1 (e)		16.2 (d)	13.2 (b) and (c)	14.2 (c) and (d)		21 (e)	Second
Right to lodge a complaint with a supervisory authority				13.2 (d)	14.2 (e)			
Whether communication is a statutory or contractual requirement, or is necessary to enter into a contract, and whether the subject is required to provide his or her personal data and the consequences of a failure to do so				13.2 (e)				
Existence of automated decision-making, including profiling, meaningful information about the logic involved, and the significance and envisaged consequences of such processing				13.2 (f)	14.2 (g)			
Information on the purpose when further processing is planned for a purpose other than that for which the data were collected				13.3	14.4			
Contact details of the data protection officer				13.1 (b)	14.1 (b)			
Period of storage or criteria used to determine that period				13.2 (a)	14.2 (a)			
Whether communications or transfers are planned and the regulations authorizing such communications or transfers				13.1 (f)	14.1 (f)			
Information to be transmitted								
Purposes of transfers			16.2 (c)					

47. As shown, among the seven international regulatory documents analysed, the United Nations Guidelines do not mention the principle of transparency. The analysis below therefore focuses on recurring references, in the remaining six documents, to information whose provision to data subjects is identified as necessary in order to uphold the principle of transparency.

48. In all six documents, it is indicated that the identities and addresses of controllers or of their representatives, and the aims or purposes of the processing, must be disclosed. These data are the basic foundations of transparency.

49. In five documents, it is stated that the rights of the data subject and the ways in they may be exercised, as well as the recipients or category of recipients, must be disclosed. With regard to the need for the subject to have information regarding his or her rights as such, reference is made to the importance of the subject being in an appropriate position to exercise control over personal information concerning him or her.

50. In three documents, it is stated that the legal foundation or basis for the processing, as well as the existence and/or main characteristics of the processing, must be disclosed.

51. The principle of transparency must be observed regardless of the legal basis for the processing. Exceptions may arise with regard to the timeliness with which information is provided to the data subject,[15] or when the data subject is not the source from which the personal information is being collected,[16] but such exceptions must be made with a view to ensuring the greatest possible transparency, as well as fairness.

52. In two documents, it is stated that the category of data processed and the origin of the data when not obtained directly from the subject must be disclosed.

53. The present analysis also includes information that is only identified in one international regulatory document as needing to be communicated to the data subject, in order to provide that subject with better conditions under which to exercise his or her power of control.

54. Such is the case of the Ibero-American Standards, in relation to the purposes of transfers, and of the General Regulation, in relation to the following information: the contact details of the data protection officer; the period of storage or criteria used to determine that period; whether communications or transfers are planned and the regulations authorizing such communications or transfers; the right to lodge a complaint with a supervisory authority; whether communication is a statutory or contractual requirement, or is necessary to enter into a contract, and whether the subject is required to provide his or her personal data and the consequences of a failure to do so; the existence of automated decision-making, including profiling, meaningful information about the logic involved, and the significance and envisaged consequences of such processing; and information on the purpose when further processing is planned for a purpose other than that for which the data were collected.

55. Among the types of information that are only included in the General Regulation, one is particularly noteworthy, namely, that aimed at ensuring that the data subject understands the way in which the information concerning him or her will be processed (whether artificial intelligence is involved, for example), and that he or

[15] Article 22 of the APEC Privacy Framework.

[16] Article 8.3 of modernized Convention 108.

she is provided with “meaningful information about the logic involved” and “the significance and the envisaged consequences”.[17]

56. The information of which the data subject must be aware, under the principle of transparency, must be provided in simple, clear, intelligible and easily accessible and understandable language;[18] special care must be taken in that regard in the case of children and adolescents.[19]

57. The proper conduct of controllers when managing personal information is also of particular importance, as they must have transparent policies for the processing of personal data.[20]

Principle of purpose

58. The principle of purpose guides and delimits all personal data processing activities, from collection to deletion. As a rule, the purpose will be defined by the data controller. However, the controller will not be considered as such if that party does not have legitimate grounds to process the data.

59. From the collection phase on, the purpose must fulfil certain characteristics, which are set out in the international regulatory documents analysed. The purpose must be explicit, specific, legitimate and relevant. Once the characteristics established in the regulations for defining the purpose or purposes have been fulfilled, they function as delimiters of the processing activities that the personal data will undergo.

60. In accordance with the principle of purpose, the data collected may be used exclusively within the limits of the purpose for which they were gathered. This principle serves to put limits on the various processing activities, from collection to storage, modification, communication, transfer and any other processing activity, up to the deletion of the data.

61. Thus, as indicated in the various regulatory documents,[21] no processing activity may go beyond what is permitted for the purposes initially defined, except as expressly authorized under the applicable regulations and in accordance with the necessary safeguards. An example of this can be found in the APEC Privacy Framework,[22] in which reference is made to the possibility of data being used for other purposes that are compatible with the purposes initially established.

62. In all of the texts analysed,[23] the principle of purpose is established and its characteristics and the consequences of its practical application are set out. This principle is closely related to the principle of legality or lawfulness, as it establishes legitimacy as an essential characteristic of the purposes.

---

[17] Data Protection Agency of Spain. *Alignment of processing operations involving artificial intelligence with the General Data Protection Regulation: an introduction.* February 2020, p. 24. Available at: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf.

[18] Article 16.3 of the Ibero-American Standards; article 12.1 of the General Regulation; article 21 of the APEC Privacy Framework.

[19] Article 16.3 of the Ibero-American Standards; article 12.1 of the General Regulation.

[20] Article 16.4 of the Ibero-American Standards; article 12 of the OECD Guidelines; article 21 of the APEC Privacy Framework.

[21] Article 5.4 (b) of modernized Convention 108; article 3 of the United Nations Guidelines; article 17 of the Ibero-American Standards; article 5.1 (b) of the General Regulation; paragraph 9 of the OECD Guidelines; articles 24 and 25 of the APEC Privacy Framework; First Principle of the OAS Principles.

[22] Part IV, article 25, of the APEC Privacy Framework.

[23] Article 54 (b) of modernized Convention 108; article 3 of the United Nations Guidelines; article 17 of the Ibero-American Standards; article 5.1 (b) of the General Regulation; article 9 of the OECD Guidelines; articles 24 and 25 of the APEC Privacy Framework; First Principle of the OAS Principles.

63. The international regulatory documents indicate which characteristics the purpose must fulfil in order for data processing to be permissible. As indicated in the table below, the purposes must be explicit, specific, legitimate and relevant.

Table 4
Characteristics of purpose

	Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data	*United Nations Guidelines for the regulation of computerized personal data files*	*Standards for Personal Data Protection of the Ibero-American Data Protection Network*	*General Data Protection Regulation of the European Union*	*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*	*APEC Privacy Framework*	*OAS Updated Principles on Privacy and Personal Data Protection, with annotations*
	Article(s)	*Article(s)*	*Article(s)*	*Article(s)*	*Paragraph*	*Principle*	*Principle*
Explicit	5.4 (b)	3	17	5.1 (b)	9	24 and 25	First
Specific	5.4 (b)	3	17	5.1 (b)	9	24 and 25	
Legitimate	5.4 (b)	3	17	5.1 (b)		24 and 25	First
Relevant	5.4 (b)	3	17	5.1 (b)	9	24 and 25	

64. Of the above-mentioned provisions, only paragraph 9 of the OECD Guidelines does not include legitimacy as a characteristic of the purposes of data processing. This may be either the result of a simple drafting issue or the omission of something that, based on the analysis of the entire regulatory document, seems to be implicit.

65. With regard to the OAS Principles, while the characteristics of purpose are not all expressly set out in the text of the First Principle, it is clear from the annotation to that Principle that they are all included under it.

66. With regard to the specificity of processing in relation to the purpose, it should be noted that the General Regulation (art. 5.1), the Ibero-American Standards (art. 17.3), modernized Convention 108 (art. 5.4 (b)) and the OAS Principles (Fourth Principle) provide for the possibility of using data for purposes other than those for which they were collected, provided that such purposes are statistical, historical or scientific.

67. As indicated above, the legitimate purpose or purposes that provided grounds for the processing delimit the actions of the controller and of the processor, if there is one. Therefore, once the purpose has been exhausted or achieved, it is no longer legitimate to continue processing the data, unless such processing is expressly provided for in the applicable regulations, in which case such provision serves as the new permissible grounds.

Principle of fairness

68. This principle concerns the need for the processing of personal information to be carried out in faithful compliance with all the terms and conditions that provided grounds for its collection and using processing methods that facilitate this objective.

69. The following is an analysis concerning the international regulatory documents that provide for this principle.

70. Article 1 of the United Nations Guidelines provides for the principle of lawfulness and fairness. The aim is to ensure that data are not processed in an unlawful or unfair way and that they are not used for ends contrary to the principles of the Charter of the United Nations. In general terms, this means that there should be no arbitrary discrimination against the data subject; that data processing should be

carried out in accordance with national and international principles and rules; and that the rights of individuals should be faithfully respected.

71. In the Ibero-American Standards, this is the “loyalty principle” (art. 15). According to that article, the controller has an obligation to privilege the protection of the subject’s interests and refrain from processing the data through deceiving or fraudulent means. Processing of personal data that results in unfair or arbitrary discrimination against subjects is considered unfair.

72. Similarly, article 5.1 (a) of the General Regulation establishes that the principle of fairness must be followed in the processing of personal data, together with the principles of lawfulness and transparency in relation to the data subject.

73. In the OECD Guidelines, fairness is referred to under the collection limitation principle (para. 7). This article addresses two issues: (a) limits to the collection of data; and (b) requirements relating to data collection methods, in connection with which it is specified that data should be obtained by lawful and fair means.

74. The principle of fairness is alluded to in article 24 of the APEC Privacy Framework, which provides that means of collection should be lawful and fair.

75. Similarly, while the principle is not expressly mentioned in modernized Convention 108, its establishment may be inferred through the provision in article 5.4 (a) that, while undergoing processing, data shall be used fairly. This condition does not apply only to the first processing activity – collection – but to any activity involving the processing of data.

76. Lastly, in the OAS Principles, the principle is established as part of the First Principle, “lawful purposes and loyalty”, according to which “personal data should be collected only for lawful purposes and by loyal and lawful means”. In this case, fairness is expressly provided for in relation to the means used for the collection of personal data.

77. In the OAS Principles, it is stated that “loyalty is contextual and depends on the circumstances”, that individuals must be provided appropriate choices about how and when they provide personal data, and that data may not be obtained by means of fraud, deception or under false pretences.

78. Fairness must be present in all personal data processing activities. In the international regulatory documents with an emphasis on collection, it is highlighted that incorrect or unlawful initial action can mark and define subsequent processing activities.

79. There should be no doubt that the actions of the controller and processor must be characterized by fair processing throughout the life cycle of personal data, regardless of the context or the technology used. Acting fairly involves responsibility, ethics and observance of the rules applicable in the light of the principles.

Principle of proportionality

80. The principle of proportionality imposes limitations on the processing of personal data. By virtue of this principle, personal data, and the processing activities that such data undergo, must be solely for the fulfilment of the purposes for which the data were collected.[24]

[24] Articles 5.1 and 5.4 (c) of modernized Convention 108; article 18.1 of the Ibero-American Standards; article 24 of the APEC Privacy Framework; article 5.1 (c) of the General Regulation; article 3 (a) of the United Nations Guidelines; paragraph 9 of the OECD Guidelines; Third and Fourth Principles of the OAS Principles.

81. It must be borne in mind that this principle must be respected at all stages of processing, from as early as the time when the decision as to whether or not to carry out the processing is taken, with a view to ensuring that the process is proper and lawful from the beginning of the collection phase.

82. Closely linked to this principle are the principle of purpose, pursuant to which data should be processed in a manner compatible with the purpose for which they were collected, and the principle of minimization, in accordance with which data should be kept to the minimum required for the achievement of the established purpose.

83. One requirement of the principle of proportionality is that the controller must conduct an evaluation in order to choose, from among the various processing operations that could be used to fulfil the authorized purpose, the one that is least invasive in terms of privacy. Such an evaluation becomes particularly necessary when it comes to the use of certain information and communications technologies that may pose a risk to fundamental rights.

84. This principle is provided for in all the international regulatory documents analysed, either specifically, as in article 18 of the Ibero-American Standards, or under other principles. It is covered under the principle of purpose-specification in the United Nations Guidelines (art. 3 (a)); under the principle of legitimacy of data processing and quality of data in modernized Convention 108 (arts. 5.1 and 5.4 (c)); as part of the principle of minimization in the General Regulation (art. 5.1 (c)); under the principle of collection limitation in the APEC Privacy Framework (art. 24); under the purpose specification principle in the OECD Guidelines (para. 9); and under the principle of relevance and necessity (Third Principle) and the principle of limited processing and retention (Fourth Principle) in the OAS Principles.

85. It can be seen from table 5 that in the Ibero-American Standards, the General Regulation, the United Nations Guidelines and the OAS Principles, reference is made to the relevance of data with regard to the purpose. Furthermore, in modernized Convention 108, the Ibero-American Standards, the General Regulation and the OAS Principles, it is stated that data must be appropriate for the purpose.

86. In all the international regulatory documents analysed, with the exception of the United Nations Guidelines, it is established, in one way or another, that data should be limited and that they should not be excessive with regard to the purpose for which they were collected. In the Ibero-American Standards, the General Regulation, the APEC Privacy Framework and the OAS Principles, it is established that data should be limited to what is necessary with regard to the purpose.

87. In modernized Convention 108, it is stated that data must not be excessive in relation to the purposes for which they are being processed. It is also stated that data must be relevant in relation to the purpose and that data processing must be proportionate in relation to the legitimate purpose pursued. In the OECD Guidelines, it is stated that the use of data should be limited to the fulfilment of the purposes specified at the time of data collection or such others as are not incompatible with those purposes.

Table 5
Limitations that shape the principle of proportionality

	Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data	*United Nations Guidelines for the regulation of computerized personal data files*	*Standards for Personal Data Protection of the Ibero-American Data Protection Network*	*General Data Protection Regulation of the European Union*	*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*	*APEC Privacy Framework*	*OAS Updated Principles on Privacy and Personal Data Protection, with annotations*
	Article	*Article*	*Article*	*Article*	*Paragraph*	*Principle*	*Principle*
Appropriate for the purpose	5.4 (c)		18.1	5.1 (c)			Third
Relevant/pertinent to the purpose	5.4 (c)	3 (a)	18.1	5.1 (c)			Third
Limited and not excessive with regard to the purpose	5.4 (c)		18.1	5.1 (c)	9	24	Third

88. In some of the international regulatory documents, such as the Ibero-American Standards, the APEC Privacy Framework, the General Regulation and the United Nations Guidelines, “personal data” is referred to expressly in the context of this principle. In others, such as the OECD Guidelines, reference is made to the “processing” of such data, while still others, such as modernized Convention 108 and the OAS Principles, contain references to both the personal data themselves and the processing that they will undergo.

89. Notwithstanding the foregoing, and taking into account the full texts of the international regulatory documents as a whole, the principle of proportionality must be viewed both in relation to the personal data collected and to the processing activities to which such data will be subject. Both the data and the processing must be appropriate, relevant, pertinent and limited to the legitimate purposes of the collection.

Principle of minimization

90. Minimization is the principle whereby data must, at all times, be limited to what is required for the achievement of the established purpose.

91. In that regard, the principle is closely linked to the principle of purpose, which serves as a parameter for limiting the amount of data to be processed.

92. The General Regulation is the only instrument that specifically establishes the principle of minimization. In its article 5.1 (c), it provides that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In the other documents analysed,[25] the content of this principle is included as part of the principle of proportionality or some other principle.

93. The principle of minimization is also related to certain obligations that the General Regulation establishes for the controller and the processor, such as privacy by design and by default. Minimization, as a preventive measure, helps to reduce the risk of security breaches and their impact with regard to databases.

[25] Article 18 of the Ibero-American Standards; article 3 of the United Nations Guidelines; articles 5.1 and 5.4 (c) of modernized Convention 108; article 24 of the APEC Privacy Framework; paragraph 9 of the OECD Guidelines; Third and Fourth Principles of the OAS Principles.

94. As stated in article 25.2 of the General Regulation, “the controller shall implement appropriate technical and organizational 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”.

95. The principle of minimization must be adhered to with greater zeal, given the increasingly frequent use of information and communications technology for the processing of personal data.

Principle of quality

96. The principle of quality requires that data be accurate, precise, complete and up-to-date, which means that data controllers must have measures in place to ensure that they are so. This principle is referred to in some international regulatory documents as the principle of accuracy[26] or completeness.[27]

97. As indicated in table 6 below, personal data must be accurate, complete and precise throughout the processing process and must be updated whenever necessary, either unprompted – by the controller or processor – or at the request of the data subject.

Table 6
Characteristics of data quality

	Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data	*United Nations Guidelines for the regulation of computerized personal data files*	*Standards for Personal Data Protection of the Ibero-American Data Protection Network*	*General Data Protection Regulation*	*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*	*APEC Privacy Framework*	*OAS Updated Principles on Privacy and Personal Data Protection, with annotations*
	Article(s)	*Article(s)*	*Article(s)*	*Article(s)*	*Paragraph*	*Principle*	*Principle*
Accurate/precise	5.4 (d)	2	19.1	5.1 (d)	8	27	Seventh
Up-to-date	5.4 (d)	2	19.1	5.1 (d)	8	27	Seventh
Complete		2	19.1		8	27	Seventh

98. In article 5.4 (d) of modernized Convention 108, it is stated that data must be accurate and kept up-to-date. Article 2 of the United Nations Guidelines refers to the obligation to check the accuracy and relevance of data; to ensure that they continue to be as complete as possible, in order to avoid errors of omission; and to ensure that they are updated regularly.

99. As indicated below, the principle of quality is expressly linked to the principle of purpose in five of the international regulatory documents.

100. Article 19 of the Ibero-American Standards establishes the obligation for the controller to adopt “the necessary measures in order to keep the personal data ... accurate, complete and updated, in such way that the veracity thereof is not altered, as required for compliance with the purposes that gave rise to its treatment”.

101. In the General Regulation, it is stated that personal data shall be accurate and, where necessary, kept up-to-date, and that every reasonable step must be taken to

[26] Article 2 of the United Nations Guidelines and Seventh Principle of the OAS Principles.
[27] Article 27 of the APEC Privacy Framework.

ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified (art. 5.1 (d)).

102. In both the OECD Guidelines (para. 8) and the APEC Privacy Framework (art. 27), reference is made to the fact that data should be accurate, complete and kept up-to-date. In the OAS Principles, it is established, in relation to the principle of accuracy of data, that "data should be kept accurate, complete and up-to-date to the extent necessary for the purposes for which it was processed, in such a way that its veracity is not affected" (Seventh Principle).

103. The quality of the personal information being processed is vital for the proper achievement of the purposes that provided grounds for the collection of that information, as well as for its subsequent processing. Ensuring the quality of data is a sign of responsibility in the pursuit of the authorized purposes.

104. In order to duly comply with the principle of quality, data controllers and processors must implement, within their organizations, measures aimed at ensuring that the personal data that they collect and manage are accurate, precise, complete or full, and up-to-date, with a view to fulfilling the authorized purposes while giving due respect to the rights of the subjects of the personal data; this will be to their own benefit. This is to be done regardless of any actions that the data subject may decide to take with the aim of ensuring the quality information of his or hers that is being processed by someone else.

Principle of responsibility

105. The principle of responsibility can be analysed from two perspectives: first, controllers and processors must put in place mechanisms to comply with privacy and data protection principles, safeguarding and guaranteeing the rights and freedoms of data subjects; second, controllers and processors must be able to guarantee and demonstrate compliance with these principles.

106. With regard to the international regulatory documents analysed, the Ibero-American Standards establish the principle of responsibility (art. 20); under that article, controllers must put in place all necessary mechanisms required to comply with the principles and obligations set forth in those Standards, and are accountable to the data subjects and the supervisory authority for the processing of personal data. To that end, controllers may make use of standards, national or international best practices, self-regulation or certification schemes, or any other mechanism they deem appropriate. The above also applies during data processing by processors and during data transfer.

107. Examples of mechanisms that controllers can adopt to comply with the principle of responsibility are listed in article 20.3 of the Ibero-American Standards. Controllers should review and evaluate such mechanisms on an ongoing basis in order to assess their effectiveness in ensuring compliance with the applicable national laws.

108. This principle is established in the General Regulation under the term "accountability" (art. 5.2). It can be defined as the need or obligation for the controller to implement appropriate technical and organizational measures to ensure and demonstrate that the processing of personal data is performed in accordance with the Regulation (art. 24), in particular the principles of lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; and integrity and confidentiality. To that end, the controller shall establish procedures to ensure the application of the rules and be able to demonstrate to third parties the effective application of and compliance with the Regulation (art. 5.2).

109. The General Regulation sets out a number of measures for ensuring compliance with this principle, including implementing data protection by design and by default

(art. 25); maintaining a record of processing activities (art. 30); implementing security measures (art. 32); notifying the supervisory authority and the data subjects of security breaches (arts. 33 and 34); carrying out a data protection impact assessment (art. 35); and designating a data protection officer (art. 37).

110. Of the above-mentioned measures, a data protection impact assessment, as provided for in the General Regulation, is required (art. 35, paras. 1, 3 and 4) when processing presents a high risk to the rights and freedoms of data subjects.[28] This is particularly relevant when new technology is used to process the data of natural persons.

111. The assessment must be carried out by the controller prior to the processing of personal data, in order to aid relevant decision-making and in line with data protection by design and by default.[29]

112. The principle of accountability requires organizations to analyse the types of data they process, the purposes of the processing and the types of processing operations performed. Based on this information, they must expressly determine how they will implement the measures required by the General Regulation, ensuring that these measures and procedures are adequate to comply with data protection requirements, and how they will demonstrate compliance to the data subjects and the supervisory authority. This principle requires organizations to take a responsible, diligent and proactive attitude with regard to all personal data processing operations they perform.[30]

113. Along the same lines, the OAS Principles emphasize the need to adopt, implement and demonstrate security measures, with a focus on accountability for the security of personal data and international data communication and transfer, with controllers assuming responsibility for assuring a continuing level of protection consistent with these Principles (Tenth Principle).

114. In the OECD Guidelines, it is stated that controllers are accountable for complying with privacy protection rules and decisions and must follow the principles established in the Guidelines (art. 14).

115. The APEC Privacy Framework also addresses the principle, focusing primarily on data transfer (art. 32). When personal information is to be transferred to another person or organization, whether domestically or internationally, the controller should obtain the consent of the data subject or, when not obtaining consent, should ensure that the recipient will protect the information consistently, and should take reasonable steps to ensure that the information is protected after it is transferred, in accordance with the principles.

116. In modernized Convention 108, it is stated that controllers and processors must implement technical and organizational measures that take into account the

[28] General Regulation, art. 35.3: “A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in article 9(1), or of personal data relating to criminal convictions and offences referred to in article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale.”

[29] Guidelines on data protection impact assessments and how to determine whether processing is “likely to result in a high risk” for the purposes of Regulation (EU) 2016/679, WP.248. April 2017. Page 16.

[30] Data Protection Agency of Spain, “What is the principle of proactive responsibility?”, www.aepd.es/es/preguntas-frecuentes/2-rgpd/3-principios-relativos-al-tratamiento/FAQ-0208-que-es-el-prinipio-de-responsabilidad-proactiva.

implications of the right to the protection of personal data at all stages of processing (arts. 10.1 and 10.3). The explanatory report to the Convention lists measures that controllers and processors may have to take, including training employees; setting up appropriate notification procedures; indicating when data have to be deleted; establishing specific contractual provisions where the processing is delegated in order to give effect to the Convention; and setting up internal procedures to enable the verification and demonstration of compliance.[31]

117. All the international regulatory documents analysed specifically address the principle, with the exception of the United Nations Guidelines. Only the Ibero-American Standards and the General Regulation establish mechanisms or measures to be adopted to ensure compliance with the principle, as shown in table 7 below.

Table 7
Principle of responsibility and mechanisms to ensure compliance

	Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data	*United Nations Guidelines for the regulation of computerized personal data files*	*Standards for Personal Data Protection of the Ibero-American Data Protection Network*	*General Data Protection Regulation of the European Union*	*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*	*APEC Privacy Framework*	*OAS Updated Principles on Privacy and Personal Data Protection, with annotations*
	Article(s)	*Article(s)*	*Article(s)*	*Article(s)*	*Paragraph*	*Principle*	*Principle*
Specifically addresses the principle of responsibility	10.1		20	5.2	14	32	Tenth
Establishes mechanisms or measures to be adopted to ensure compliance with the principle			20.3	5.1, 24, 25, 30, 32, 33, 34, 35 and 37			

118. Essentially, the principle of responsibility tends to strengthen compliance with the data protection and privacy principles and regulations that controllers and processors have to observe in all processing activities carried out, and ensure that objective elements underpin genuine compliance and the fulfilment of legitimate purposes, in a climate of trust and respect for the fundamental rights involved.

Principle of security

119. Security is fundamental to data protection; there can be no data protection without security.

120. To ensure compliance with this principle, the risks that can arise during the life cycle of personal data must be identified, evaluated and documented, in order to implement the necessary security measures and be able to guarantee the confidentiality, integrity and availability of personal data, avoiding any risks.

121. All the international regulatory documents analysed address this principle, in a more or less descriptive manner, and note the need to establish appropriate, sufficient, timely, reasonable or adequate security measures to prevent various types of risk, such

[31] Explanatory report to the Convention, article 10, para. 85. Available at: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.

as unauthorized access and the loss, alteration, destruction or disclosure of personal data.[32]

122. Table 8 lists the types of security measures and risks referred to in each of the international regulatory documents. The table also indicates which documents contain guidelines for determining the measures to be taken and which establish the obligation to report security breaches.

Table 8
Principle of security

	Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data	*United Nations Guidelines for the regulation of computerized personal data files*	*Standards for Personal Data Protection of the Ibero-American Data Protection Network*	*General Data Protection Regulation of the European Union*	*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*	*APEC Privacy Framework*	*OAS Updated Principles on Privacy and Personal Data Protection, with annotation*
Type of security measure	Appropriate security measures (art. 7.1)	Appropriate measures (art. 7)	Sufficient administrative, physical and technical measures (art. 21.1)	Appropriate technical or organizational measures (art. 5.1 (f))	Reasonable security safeguards (para. 11)	Appropriate safeguards (art. 28)	Reasonable and appropriate technical, administrative or organizational security safeguards (Sixth Principle)
Type of risk	Accidental or unauthorized access, destruction, loss, use, alteration or dissemination of personal data (art. 7.1)	Natural dangers, such as accidental loss or destruction, and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses (art. 7)	Damage, loss, alteration, destruction, access and, in general, any illegal or non-authorized use of personal data (art. 22.1)	Unauthorized or unlawful processing and accidental loss, destruction or damage (art. 5.1 (f))	Loss or unauthorized access, destruction, use, modification or disclosure of data (para. 11)	Loss or unauthorized access, or unauthorized destruction, use, modification or disclosure or other misuses (art. 28)	Unauthorized or unlawful processing, including access, loss, destruction, damage or disclosure, even when accidental (Sixth Principle)
Guidelines for determining what measures to take			art. 21.2	art. 32		art. 28	
Notification of security breaches to the supervisory authority	art. 7.2		art. 22	art. 33	para. 15 (c)	art. 54	
Notification of security breaches to data subjects			art. 22.	art. 34	para. 15 (c)	art. 54	

[32] This information is presented in table 8, which sets out the types of security measures and risks referred to in the provisions cited therein (article 7.1 of modernized Convention 108; article 7 of the United Nations Guidelines; article 21.1 of the Ibero-American Standards; article 5.1 (f) of the General Regulation; paragraph 11 of the OECD Guidelines; article 28 of the APEC Privacy Framework; and the Sixth Principle of the OAS Principles).

123. Security measures must be proportional to the magnitude of the risk; they should be reviewed and updated periodically, and may also be audited, to improve them and prevent them from becoming obsolete.[33]

124. In the OAS Principles, it is stated that security measures should be permanently audited and updated (Sixth Principle), while in the Ibero-American Standards, it is stated that the controller shall perform actions that guarantee the monitoring, revision, maintenance and continuous improvement of the security measures applicable to the treatment of personal data, in a periodic way (art. 21.3). In the APEC Privacy Framework, it is stated that security measures should be subject to periodic review and reassessment (art. 28).

125. Various international regulatory documents cover the obligation to notify the supervisory authority of security breaches, including modernized Convention 108 (art. 7.2), the Ibero-American Standards (art. 22), the General Regulation (art. 33), the OECD Guidelines (para. 15 (c)) and the APEC Privacy Framework (art. 54). With the exception of modernized Convention 108, these documents also establish the obligation to communicate security breaches to the data subjects concerned.

126. The importance of notifying the supervisory authority and, where appropriate, the data subjects must be emphasized. This allows the supervisory authority to ensure that appropriate measures are taken in the event of a security breach and that the breach is contained as quickly as possible; it also ensures that the data subjects affected by the security breach are aware of the breach and the harm that could be caused as a result.

127. The Data Protection Agency of Spain notes that according to the principle of security in the General Regulation, those who process data are required to carry out a risk analysis to determine the technical and organizational measures that need to be implemented to guarantee the integrity, availability and confidentiality of the personal data they process.[34]

128. The Ibero-American Standards (art. 21.2), the General Regulation (art. 32) and the APEC Privacy Framework (art. 28) set out guidelines or factors for determining the security measures that should be implemented, as discussed below, but none of them stipulates the specific measures to be taken, since it would be impossible to do so in a way that did not become obsolete.

129. In the General Regulation, it is stated that the controller and the processor shall take into account the following factors when determining appropriate measures to ensure a level of security appropriate to the risk: “the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons” (art. 32).

130. The Ibero-American Standards also refer to these factors, and add the following: international transfers of personal data carried out or to be carried out; the number of data subjects; the possible consequences of a data breach for data subjects; and previous breaches (art. 21.2).

131. In the APEC Privacy Framework, it is stated that security measures should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held (art. 28). Under the Privacy Framework, unlike the other international regulatory documents, only the controller

[33] Sixth Principle of the OAS Principles.

[34] Data Protection Agency of Spain, “Principles”, 25 November 2021, www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios.

is responsible for implementing and maintaining security measures based on the factors mentioned above, with no mention of the processor.

132. In the OAS Principles, the principle of security is not articulated in the way indicated above. Nevertheless, they state that “the measures adopted to protect personal data should be chosen in consideration of, among other factors, (i) their possible effect on the rights of data subjects, particularly the potential value that unauthorized third parties may find in the data; (ii) the costs associated with their implementation; (iii) the purposes for processing; and (iv) the nature of the personal data being processed, especially sensitive data” (Sixth Principle, annotation).

133. Of the international regulatory documents analysed, only the General Regulation provides examples of technical and organizational measures to ensure a level of security appropriate to the risk, namely: “(a) the pseudonymization and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing” (art. 32.1).

134. Article 32.3 of the General Regulation states that adherence to a code of conduct or a certification mechanism may be used to demonstrate compliance with these requirements.

135. All controllers and processors must take measures to ensure the security of and protect personal data against risks such as unauthorized access, loss, alteration, destruction, disclosure or damage. If security measures are not taken, personal information is vulnerable to these risks, which may result in serious harm to the rights of data subjects. For this reason, all the international regulatory documents analysed address the need to establish various types of measures against the risks that could arise; in some cases, they even provide guidelines for determining the appropriate security measures to take, although they do not specify exact measures, given that it would be impossible to update the documents to keep pace with technological advances and possible violations.

136. The variety of technologies and their dynamic transformation, which increases their capacity to collect and process data, must be taken into account in order to evaluate in a responsible and ethical manner the risks and the appropriate security measures to be taken by data controllers, in the context of their legitimate authorization as such, as well as the unquestionable need to preserve the due confidentiality of the personal data being processed under their responsibility.

137. To avoid serious violations of the rights of data subjects, it is essential to ensure the integrity, availability and confidentiality of personal data, responsibility for which falls on data controllers and processors. Should breaches occur, they should have the smallest possible impact on the rights of data subjects; guidelines to be followed when breaches occur, such as the requirement to notify the supervisory authority and the data subjects concerned, must be established.

III. Conclusion

138. The guiding principles underpinning privacy and personal data protection are a structural part of the legal systems relating to those issues. Those principles serve as guidelines for interpretation, help to fill gaps in the law and require controllers and processors to act appropriately in processing personal data.

139. Legality must be the foundation for all processing activities throughout the life cycle of personal data and is based on the existence of legitimate grounds, as established in the applicable regulations.

140. The principle of consent is closely linked to the principle of legality, as it is the most common internationally recognized permissible grounds for the processing of personal data.

141. The principle of transparency must be observed regardless of the legal basis for the processing.

142. The principle of purpose is established in all the regulatory documents analysed. The purpose must be explicit, specific, legitimate and relevant. It functions as a delimiter of the processing activities that the personal data will undergo.

143. The principle of fairness requires that personal information be processed in faithful compliance with all the terms and conditions that provided grounds for its collection and using processing methods that facilitate this objective.

144. In accordance with the principle of proportionality, the use of personal data, and the processing activities that such data undergo, must be solely for the fulfilment of the legitimate purposes for which the data were collected.

145. The quality of the personal information being processed is vital for the proper achievement of the purposes that provided grounds for the collection of that information, as well as for its subsequent processing.

146. The principle of responsibility tends to strengthen compliance with principles and regulations, and ensure that objective elements underpin genuine compliance and the fulfilment of legitimate purposes, in a climate of trust and respect for the fundamental rights involved.

147. There can be neither data protection nor respect for privacy without security. Ensuring the integrity, availability and confidentiality of personal data is an essential task and a major responsibility. The variety of technologies and their dynamic transformation must be taken into account in order to evaluate risks and appropriate security measures in a responsible and ethical manner.

148. There are many commonalities in how the international regulatory documents address the principles of privacy and personal data protection.

149. The common elements identified could serve as a basis for moving towards a global consensus that will make it possible to address, in a concerted and appropriate manner, the various challenges that arise in the processing of personal data, such as international data transfers, the use of information and communications technology and artificial intelligence; human rights deserve equal respect in virtual and in face-to-face environments.

150. It is necessary to continue making progress towards finding a balance between the different interests involved in the processing of personal data in the current global and digital era, in pursuit of regulatory cooperation and harmonization.