United Nations A/79/173

General Assembly

Distr.: General
17 July 2024
English
Original: Spanish

Seventy-ninth session
Item 71 (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.

* A/79/150.

24-13146 (E) 020824 080824

Report of the Special Rapporteur on the right to privacy, Ana Brian Nougrères

Proposal for the updating of General Assembly resolution 45/95 of 14 December 1990, entitled “Guidelines for the regulation of computerized personal data files”

Summary

In the present report, the Special Rapporteur on the right to privacy sets out a proposal for the updating of General Assembly resolution 45/95 of 14 December 1990, entitled “Guidelines for the regulation of computerized personal data files”, in order to update its content to bring it into line with the socio-technological reality of the twenty-first century.

I. Background and justification

1. In accordance with the Charter of the United Nations, signed on 26 June 1945,[1] one of the objectives of the United Nations is "to achieve international co-operation ... in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language or religion".[2] The rights of individuals with respect to the processing of their personal data are therefore also among the concerns of the United Nations.

2. By its resolution 45/95 of 14 December 1990, the General Assembly[3] adopted the Guidelines for the regulation of computerized data files.[4] This resolution was preceded by Commission on Human Rights resolution 1990/42 of 6 March 1990 and Economic and Social Council resolution 1990/38 of 25 May 1990, entitled "Guidelines on the use of computerized personal files". These guidelines are not legally binding on States but have been very important and have been incorporated by Governments into their domestic regulations and cited by judges and academics.

3. Resolution 45/95 was adopted in 1990 in response to the socio-technological realities of that time. Since then, new technological phenomena have arisen and advancements have been made that have transformed our society and are part of our daily lives. For example:

- The emergence and expansion of public use of the Internet have revolutionized the way in which we gain access to and share information from all over the world.
- Smartphones have become essential for communication, work, education and entertainment.
- Digital social networks have transformed online communication and social connection.
- Cloud computing has changed the way in which businesses and individuals manage information, as it allows them to gain access to and store online data and applications from around the world, from anywhere in the world.
- Big data has enabled sophisticated analysis and decision-making based on the processing of large quantities of data.
- Artificial intelligence is generating enormous expectations and changes owing to its advanced algorithms and its production of information.
- The Internet of things enables the interconnection of physical devices through the Internet and the sharing of information in order to automate and remotely control various systems.

[1] The official text of the Charter of the United Nations is available on the Organization's website: www.un.org/about-us/un-charter.

[2] Article 1, paragraph 3, of the Charter of the United Nations. Other purposes of the United Nations set forth in Article 1 are: "1. To maintain international peace and security ...; 2. To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace; 3. To achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and 4. To be a centre for harmonizing the actions of nations in the attainment of these common ends".

[3] The General Assembly is the chief deliberative, policymaking and representative organ of the United Nations (www.un.org/en/ga/about/background.shtml).

[4] The principles apply to the computerized files of public and private entities. They can also be applied, subject to certain adjustments, to manual files (see para. 10 of the Guidelines).

- Virtual reality and augmented reality have made it possible to create new digital experiences, including games, training applications and simulations.
- Advancements in artificial intelligence and sensors have enabled cars to operate independently, thereby transforming the transportation industry and the way in which people travel.
- Neurotechnology has led to detailed knowledge of the brain and information on the neural systems of individuals (highly sensitive data).

4. None of these technological developments had taken place when General Assembly resolution 45/95 was adopted. It is therefore necessary to update them in order to bring them into line with the socio-technological reality of the twenty-first century. In addition, current technology allows data to be collected anywhere in the world from individuals domiciled or residing in other countries. This phenomenon, known as "international data collection",[5] is not envisaged in General Assembly resolution 45/95. As the means by which data are most frequently collected from individuals worldwide, it should be incorporated into international documents.

5. Information is also essential to the functioning of technological tools, such as artificial intelligence, given that an algorithm, by itself, is not sufficient to produce a result; the result comes from the processing and analysis of information.

6. Personal data is a specific category of information. Such data are so valuable that they have been referred to as the "currency of the digital economy". For example, at the end of December 2022, the Organisation for Economic Co-operation and Development (OECD) adopted the Declaration on a Trusted, Sustainable and Inclusive Digital Future,[6] which highlights, among other things, "the outcomes of the OECD Horizontal Project on Data Governance for Growth and Well-being … which recognise the importance of data as a **driver of the global economy**" (emphasis added).

7. OECD has committed itself to, among other things, "advancing a human-centric and rights-oriented digital transformation that includes promoting the enjoyment of human rights, both offline and online, strong protections for personal data, laws and regulations fit for the digital age, and trustworthy, secure, responsible and sustainable use of emerging digital technologies and artificial intelligence".[7]

8. On 23 January 2023, the European Parliament, the Council of the European Union and the European Commission adopted the European Declaration on Digital Rights and Principles for the Digital Decade,[8] in whose chapter III, entitled "Freedom of choice", under the subheading "A fair digital environment", they committed themselves to, among other things, "ensuring a safe and secure digital environment based on fair competition, where fundamental rights are protected, users' rights and consumer protection in the Digital Single Market are ensured, and responsibilities of platforms, especially large players and gatekeepers, are well defined".

---

[5] Nelson Remolina Angarita, *Recolección internacional de datos personales: un reto del mundo post-internet* (Madrid, Spain, Official Gazette, 2015).

[6] Organisation for Economic Co-operation, "Declaration on a Trusted, Sustainable and Inclusive Digital Future". The Declaration was the outcome of the meeting held on the island of Gran Canaria, Spain, on 14 and 15 December 2022. The official text is available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0488.

[7] Ibid.

[8] European Parliament, Council of the European Union and European Commission, European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01), 23 January 2023. The official text is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOC_2023_023_R_0001.

9. All of the above has led to a review, across the world, of relevant international documents on data processing and of local laws, with a view to modernizing them. In that regard, in October 2023, the Global Privacy Assembly (GPA) adopted a resolution aimed at achieving global data protection standards, in which it set forth principles to ensure high levels of data protection and privacy worldwide and emphasized a decades-old idea, namely, that there should be global standards on data protection and privacy. In the resolution, GPA therefore promoted certain principles, rights and other elements as important for achieving high levels of data protection and privacy, and resolved to advocate, promulgate and promote the principles, rights and other elements set out in the resolution, to ensure that they could be effectively implemented and applied in all contexts, particularly in the processing of data with new and emerging technologies and innovations.[9]

10. In the resolution, GPA emphasized the importance of providing for the protection of personal data across borders with a range of transfer mechanisms, such as adequacy, model clauses, certifications and administrative arrangements, to ensure that protection travels with the data when the data cross borders. It also noted the benefits of building on commonalities, complementarities and elements of convergence in order to foster future interoperability between existing regulatory approaches and mechanisms enabling safe, trustworthy cross-border data flows.[10]

11. Such international regulatory harmonization began in the twentieth century, with the Council of Europe, OECD, the United Nations, the European Parliament and the Council of the European Union as the main stakeholders. In the twenty-first century, they were joined by the Asia-Pacific Economic Cooperation forum (APEC), the Ibero-American Data Protection Network and GPA, formerly known as the International Conference of Data Protection and Privacy Commissioners.

12. In that connection, the Ibero-American Data Protection Network has stated that the "establishment of a harmonized framework for data protection at the global level has been the main basis for the adoption of the various current international instruments on data protection. The aim is to ensure that the development of global commerce is compatible with the protection of the rights of individuals, especially with regard to the protection of information concerning them".[11]

13. Lastly, mention should be made of cyberspace as the milieu in which millions of people in the world coexist.

14. Personal data circulate daily in cyberspace. However, the regulation of data processing arose in an environment in which cyberspace was not yet being discussed. In other words, the current socio-technological reality is not the socio-technological reality that existed when the first regulations on personal data protection were issued.

[9] GPA, resolution entitled "Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide", October 2023. Available at https://globalprivacyassembly.org/document-archive/adopted-resolutions/.

[10] Ibid.

[11] Ibero-American Data Protection Network, "Guidelines for Harmonization of Data Protection in the Ibero-American Community", p. 1 (2007). The Ibero-American Data Protection Network goes on to state that "therefore, the establishment of a homogeneous framework for the regulation of the right to data protection, either through the adoption of binding supranational instruments or of national laws enshrining the essential content of that right, will ensure the development of commerce in the area, facilitating the exchange of information between the various operators located in the Ibero-American States and between those States and third countries, in particular the States members of the European Union, without restrictions resulting from differences in the level of protection of the fundamental right to the protection of personal data".

15. However, information and personal data are a central and indispensable part of cyberspace. Although there are different definitions of cyberspace, it should be understood as comprising the following aspects:

- Technological infrastructure (technological resources) composed of countless pieces of equipment (servers, computers, cell phones, tablets, etc.) located in many parts of the world
- A worldwide platform for communications (global communications network), information and interconnected networks (Internet), known as "global information infrastructure"
- Millions of people and organizations of diverse nationalities that are based in countries with dissimilar legal systems and that, from anywhere in the world, use technology, communications and information to interact with other people, and utilize the services available on the Internet
- Huge amounts of information (including personal data) that are constantly circulating within countries and across borders

16. Little by little, we are witnessing a shift from a physical world demarcated by geographical borders to a technological cyberspace without borders, in which the number of people interacting at any one time is gradually increasing.

17. The global, international and cross-border nature of many activities conducted through the Internet, such as e-commerce, has been a key aspect that has led to the need for appropriate regulations in order to promote development and innovation, and to sufficiently protect the right of individuals whose information is collected and used by companies, people and Governments throughout the world. In the Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind,[12] the General Assembly recognizes not only that "scientific and technological progress is of great importance in accelerating the social and economic development of developing countries", but also that, while such developments "provide ever-increasing opportunities to better the conditions of life of peoples and nations, in a number of instances they can give rise to social problems, as well as threaten the human rights and fundamental freedoms of the individual". For this reason, the Assembly continues, there is a "need to make full use of scientific and technological developments for the welfare of man and to neutralize the present and possible future harmful consequences of certain scientific and technological achievements". Consequently, the Assembly agreed, among other things, that: "all States shall take effective measures, including legislative measures, to prevent and preclude the utilization of scientific and technological achievements to the detriment of human rights and fundamental freedoms and the dignity of the human person".[13]

II. Reports of the Special Rapporteur on the right to privacy on issues relevant to the updating of General Assembly resolution 45/95

18. In a 2022 report,[14] the Special Rapporteur conducted a comparative study of seven international documents in order to determine the scope of the following principles relating to the processing of personal data: legality, lawfulness and legitimacy, consent, transparency, purpose, fairness, proportionality, minimization,

[12] General Assembly resolution 3384 (XXX) of 10 November 1975.

[13] Ibid., para. 8.

[14] "Principles underpinning privacy and the protection of personal data", report of the Special Rapporteur on the right to privacy (A/77/196, 20 July 2022).

quality, responsibility and security. She also highlighted the common aspects of the international documents in relation to the principles in order to build bridges between those documents and establish points of contact so as to facilitate harmonization at the global level.

19. She drew the following conclusions in that report:

- 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.
- 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.
- 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.
- The principle of transparency must be observed regardless of the legal basis for the processing.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- There are many commonalities in how the international regulatory documents address the principles of privacy and personal data protection.
- 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.

- 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.[15]

20. In a 2021 report on artificial intelligence and privacy, and children's privacy,[16] the Special Rapporteur provided the information described below.

21. First, with respect to children's privacy, he concluded that it was necessary, among other things, to adopt policies, laws and standards which:

- Cast children as the bearers of human rights where their rights to privacy, autonomy and equality are inalienable.
- Incorporate the broad scope of privacy, not solely data protection, to enable the full development of children's potential.
- Incorporate children's views, children's strategies for privacy, findings of child-focused research and/or child privacy impact assessments in public policy settings.
- Provide independent means to conciliate, arbitrate and remedy individual or systemic human rights violations against children and ensure that enforcement measures are taken in case of infringements.[17]

22. He also made the following recommendations:

- Ensure that biometric data is not collected from children, unless as an exceptional measure only when lawful, necessary, proportionate and fully in line with the rights of the child.
- Ensure that children's personal data is processed fairly, accurately, securely, for a specific purpose in accordance with a legitimate legal basis utilizing data protection frameworks representing best practice, such as the General Data Protection Regulation and Convention 108+.
- Ensure that those who process personal data, including parents or carers and educators, are made aware of children's right to privacy and data protection.
- Ensure that information is available to children on exercising their rights on, for example, the websites of data protection authorities, and ensure the provision of counselling, complaint mechanisms and remedies specifically for children, including for cyberbullying.
- Prohibit automated processing of personal data that profiles children for decision-making concerning the child or to analyse or predict personal preferences, behaviour and attitudes, with exemption only in exceptional circumstances in the best interests of the child or an overriding public interest, with appropriate legal safeguards.[18]

23. Second, the Special Rapporteur made recommendations on the protection of privacy in the development and implementation of artificial intelligence-based solutions, in order to "provide guiding principles concerning the use of personal and non-personal information in the context of artificial intelligence (AI) solutions developed as part of applied information and communications technologies (ICTs), and to emphasize the importance of a legitimate basis for AI data processing by

[15] Ibid., paras. 138–150.
[16] "Artificial intelligence and privacy, and children's privacy", report of the Special Rapporteur on the right to privacy (A/HRC/46/37, 25 January 2021).
[17] Ibid., para. 126.
[18] Ibid., para. 127.

Governments and corporations within the overarching framework of the human right to privacy".[19]

24. He highlighted in the report that both the processing of data through artificial intelligence-based tools and the decision made as a result of such processing have potential risks for the data subject. Therefore, he considered it important to set forth a number of principles that should be taken into account in the planning, development and implementation of artificial intelligence-based solutions, namely: (a) jurisdiction; (b) ethical and lawful basis; (c) data fundamentals; (d) responsibility and oversight; (e) control; (f) transparency and "explainability"; (g) rights of the data subject; and (h) safeguards.

25. In a subsequent report, the Special Rapporteur referred to the principles of transparency and explainability in the processing of personal data in artificial intelligence and emphasized the importance of these principles in that context.[20]

26. These principles are relevant because transparency and explainability not only help to build trust and reliability in artificial intelligence, but also contribute to the protection of human rights. These principles allow individuals affected by artificial intelligence to be informed in a timely, comprehensive, simple and clear manner about basic issues concerning the use of their personal information in artificial intelligence processes or projects and the consequences thereof, and about the specific reasons why they have been affected. This makes it possible for them to exercise their rights, such as the right to due process and to a defence when faced with decisions made using artificial intelligence tools or technologies.

27. In the report, the Special Rapporteur indicated that artificial intelligence involved different types of risk. The contingencies that should be considered include the risks inherent in operating with algorithms (human bias, technical flaws, security vulnerabilities and failures in their implementation), in their design and in the processing of personal data.

28. The Special Rapporteur also pointed out that personal data were an input processed by algorithms to produce results. Data input can be affected mainly by bias (incorporation of partial, insufficient, outdated or manipulated data) and pertinence (relevance, inconsistency or completeness of the data). If high-quality and pertinent data are not used, the results will be erroneous. Algorithms, for their part, can be affected by patterns (programming logic bias, including unforeseen functions and inherent failures of the functions used for their codification), and errors (operating conditions that reflect a method of operation that differs from the method of operation planned and goes against the premise of the proposed design). These issues have an impact on the results obtained using artificial intelligence-based tools, which are related to the pertinence and precision of the execution of the algorithms and are a result of the analysis of the data input.

29. The following were among the conclusions drawn in the report:

(a) Transparency and explainability help to build trust in artificial intelligence and to respect human rights;

(b) Developers of artificial intelligence must be transparent about how data are processed (how they are collected, stored and used), and about how decisions based on artificial intelligence are made, the reliability of such decisions and the security of the information;

[19] Ibid., para. 1.

[20] "Principles of transparency and explainability in the processing of personal data in artificial intelligence", report of the Special Rapporteur on the right to privacy (A/78/310, 30 August 2023).

(c) Persons affected by decisions made on the basis of artificial intelligence deserve a clear, simple, complete, truthful and understandable explanation of the reasons for that decision. In that regard, the principle of explainability is of cardinal importance not only because it aligns with the principle of transparency, but also because it will make it possible to uphold such persons' right to a defence and due process;

(d) Explainability and transparency demand clarity, completeness, truthfulness, impartiality and publicity of the decisions made using artificial intelligence and of the logic, method or reasoning for making decisions about human beings based on information, particularly personal data. Explainability and transparency are, of course, the opposite of opacity, obscurity, deceit, lies and abuse of computing power, which are some of the symptoms of illegal and unethical processing that reflects a lack of respect for human beings and their dignity.[21]

30. In addition, the Special Rapporteur made the following recommendations:

(a) Promote transparency in artificial intelligence in order to mitigate the risks that opacity may generate in society, especially with respect to the protection of human rights;

(b) Incorporate into [national] laws the principle of explainability, not only to enable people to understand how the decisions that affect them were made, but also to provide them with the tools to defend their human rights in the face of artificial intelligence;

(c) Promote ethical practices that ensure transparency and explainability in the processing of personal data in artificial intelligence projects or processes;

(d) Foster, support and facilitate education and digital literacy to enable citizens to better understand the concepts relating to artificial intelligence, transparency and explainability, in order to be able to demand that their rights be respected.[22]

31. In a 2024 report,[23] the Special Rapporteur conducted a comparative study of the legal safeguards for personal data protection and privacy in the digital age. She also examined the legal mechanisms that are available to data subjects for the protection and restitution of their rights and, where necessary, for the reparation of damage caused by the improper use of information concerning them.

32. The following were among the conclusions drawn in the report:

(a) Countries from five continents have expressly recognized in their legislation the different rights that data subjects enjoy and that allow them to control their personal information;

(b) Some countries are moving forward by legislating to recognize new rights, including those that are linked to automated and digitalized data processing or are exercised in the context of the Internet or of social media and similar services. This progress can also be seen from the more detailed express recognition of certain rights;

(c) Data subjects exercise personal data protection rights vis-à-vis data controllers through regulated procedures in each legal system that possess similarities and particular features;

(d) Regulated aspects of these procedures include, depending on the law in question, the ability of the data subject or his or her representative to submit requests

[21] Ibid., para. 63.

[22] Ibid., para. 64.

[23] "Legal safeguards for personal data protection and privacy in the digital age", report of the Special Rapporteur on the right to privacy (A/HRC/55/46, 18 January 2024).

for the exercise of a right; the types of possible response; the medium of the response; the deadline for responding; whether the procedure is free of charge; and, if a rights request is refused, the duty to inform the data subject of the possibility of submitting a complaint to an administrative or judicial authority;

(e) In respect of administrative remedies, which data subjects may pursue if the data controller fails or refuses to protect their rights, there is a degree of regulatory convergence. The laws of certain countries include specific provisions on the submission of complaints free of charge; on time limits for the resolution of procedures; and on the possibility of referral to alternative dispute resolution mechanisms;

(f) In all of the laws considered, provision is made for administrative measures to protect the claimed right, some of which are intended to prevent the continuation of the infringement or repetition of the conduct;

(g) Certain laws clearly establish the possibility of appealing against the decisions of the supervisory authority before a higher administrative body and the possibility of challenging the decisions of the supervisory authority before the courts in accordance with the right to effective judicial protection;

(h) In some countries, the law gives data subjects the option of whether to turn to the administrative supervisory authority or to directly approach the competent judicial body in order to seek a remedy for the protection of personal data that the data controller has refused or failed to protect;

(i) The five countries covered by the analysis regulate, to a greater or lesser extent, aspects of the redress that may be sought by data subjects who have suffered damage or loss as a result of a breach of data protection and privacy legislation.[24]

33. In her main recommendations, the Special Rapporteur urged States to:

(a) Establish and bring up to date appropriate legal frameworks, on a multidisciplinary basis and with the support of all stakeholders, in particular through the adoption of laws and regulations that provide accessible and appropriate remedies for the effective protection, reparation and restitution of the right to personal data protection, including compensation for damage caused by violations of the relevant laws and regulations;

(b) Acting in a sovereign capacity, identify and consider adopting aspects of other countries' data protection and privacy legislation that may offer stronger guarantees for the effective realization of these rights in the digital age;

(c) Promote and foster human rights information and education, particularly in the area of personal data protection and privacy, as a matter of priority, at all levels and in all fields, so that data subjects are aware of, understand and can exercise their rights and, if necessary, can avail themselves of remedies to ensure their effective enjoyment.[25]

34. In 2022, the Special Rapporteur submitted a report on the implementation of the principles of purpose limitation, deletion of data and demonstrated or proactive accountability in the processing of personal data collected by public entities in the context of the COVID-19 pandemic,[26] with a view to determining what had happened

[24] Ibid., para. 123.

[25] Ibid., para. 124.

[26] "Implementation of the principles of purpose limitation, deletion of data and demonstrated or proactive accountability in the processing of personal data collected by public entities in the context of the COVID-19 pandemic", report of the Special Rapporteur on the right to privacy (A/HRC/52/37, 27 December 2022).

and would happen to the data collected from millions of people from all countries in the world in order to combat the pandemic.

35. The Special Rapporteur drew a number of conclusions and made the following recommendations on the basis of an analysis of 20 countries in Africa, the Americas, Asia, Europe and Oceania:

- Ensure [genuine and effective compliance] with the principles of purpose limitation, deletion of data and demonstrated or proactive accountability in respect of the data of millions of people that were collected for the purpose of detecting and/or combating COVID-19 and tracking its spread with a view to protecting public health and preventing its transmission.
- Reinforce the application of the principle of demonstrated or proactive responsibility in all programmes and policies involving the processing of personal data. This requires [States], among other things, to adopt relevant, appropriate, timely and effective measures to comply with the legal obligations established in personal data processing regulations. Such measures should be subject to ongoing review and evaluation in order to gauge how effective they are in terms of ensuring compliance and the protection of personal data.
- Implement processes and use tools that demonstrate and provide evidence of due compliance with [national] obligations. Such processes and tools should be transparent and easily verifiable by the competent public authorities and the public in general.
- It is suggested that, before commencing the design and development of applications and software that involve processing personal data for the purpose of carrying out State functions, States should take proactive, preventive measures with a view to establishing a risk monitoring and management system that will ensure that data are processed fairly and lawfully.
- Cement a public culture that fosters transparent and ethical processing of personal data, with all due safeguards, so as to ensure that transparency becomes an essential component in the design and implementation of all public programmes and policies that involve the processing of personal data.
- Build and consolidate levels of public confidence in the programmes of public entities that involve the processing of personal data by implementing transparent, publicly accessible mechanisms that allow citizens to verify, through a simple process and at any time, that public entities comply in practice with the procedures and commitments set forth in their policy notices and/or terms and conditions for activities that involve the collection, use and exchange of personal data or any other activity in which personal data are processed.[27]

III. Some thematic gaps in General Assembly resolution 45/95 as compared with international documents on personal data processing

36. Because General Assembly resolution 45/95 was adopted in 1990, its content is outdated compared with that of subsequent international documents. This can be seen from a comparative analysis of the resolution and the following documents:

- APEC Privacy Framework, 2004

[27] Ibid., paras. 27–32.

- International Standards on the Protection of Personal Data and Privacy: Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the Processing of Personal Data (Madrid Resolution), 2009
- Recommendation of the OECD Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 2013
- Regulation (European Union) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Standards for Personal Data Protection for Ibero-American States,[28] adopted in 2017
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+), Council of Europe, 2018
- Updated Principles on Privacy and Personal Data Protection, Organization of American States (OAS), 2021[29]
- Resolution entitled "Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide", GPA, 2023[30]

37. The main results of the comparative analysis are set out below.

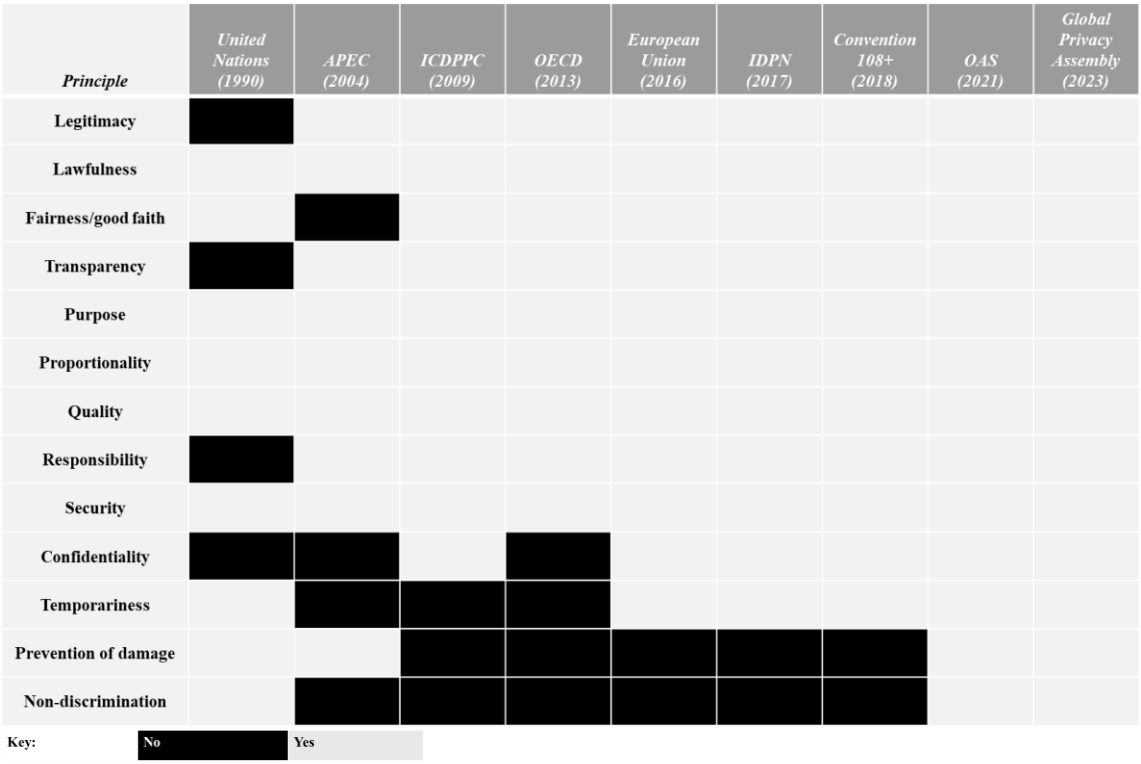
First: as indicated in the table below, in its resolution 45/95 the General Assembly does not mention the following principles relating to the processing of personal data: legitimacy, transparency, demonstrated responsibility and confidentiality.

[28] Document adopted at the fifteenth Ibero-American Data Protection Meeting of the Ibero-American Data Protection Network, held in Santiago on 22 June 2017.

[29] The Principles were adopted by the Inter-American Juridical Committee and approved by the General Assembly of the Organization of American States in 2021.

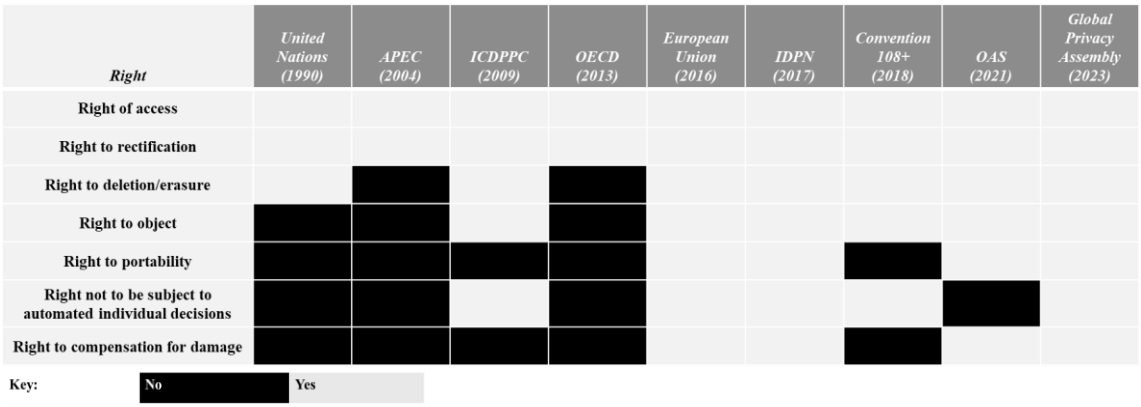
[30] See footnote 9.

Table 1
Principles relating to the processing of personal data explicitly mentioned in international documents



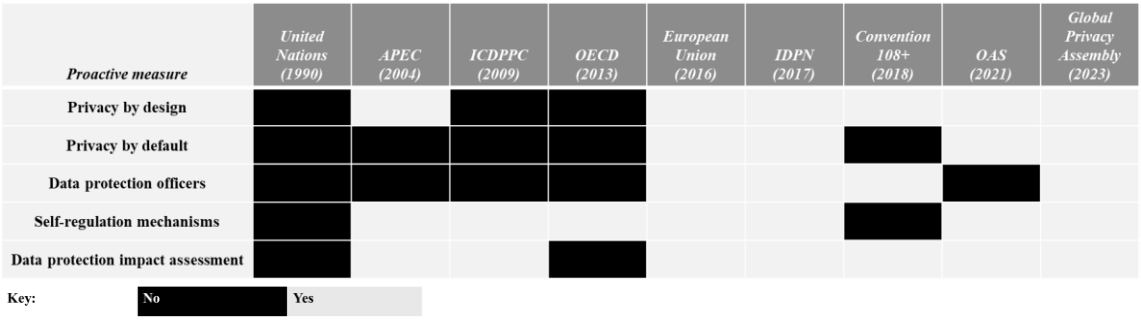
Second: as shown in the table below, in its resolution 45/95 the General Assembly does not mention the following rights of data subjects: the right to object, the right to portability, the right not to be subject to automated individual decisions, and the right to compensation for damage.

Table 2
Rights of data subjects explicitly mentioned in international documents



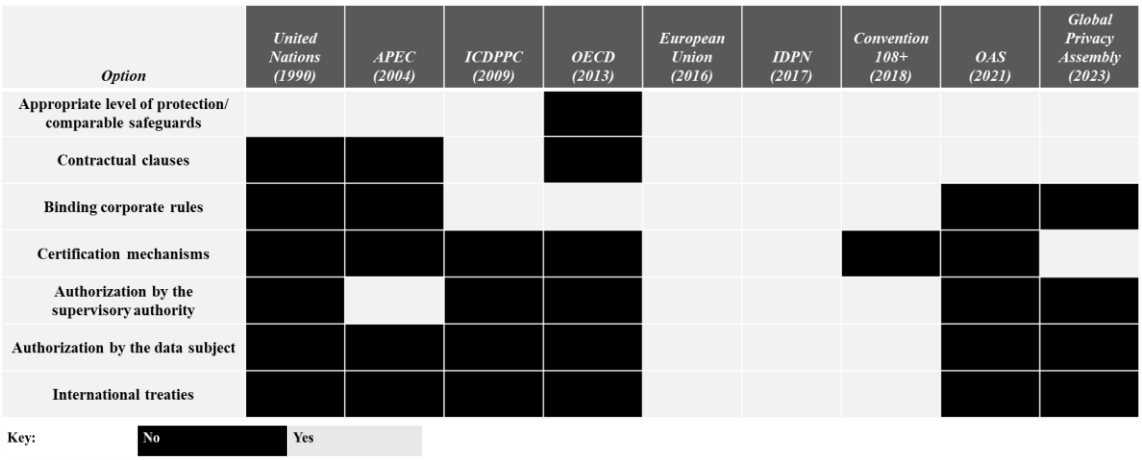
Third: as demonstrated in the table below, in its resolution 45/95 the General Assembly does not mention the following proactive measures relating to data processing: privacy by design, privacy by default, data protection officers, self-regulation mechanisms, and data protection impact assessment.

Table 3
Proactive measures relating to the processing of personal data explicitly mentioned in international documents



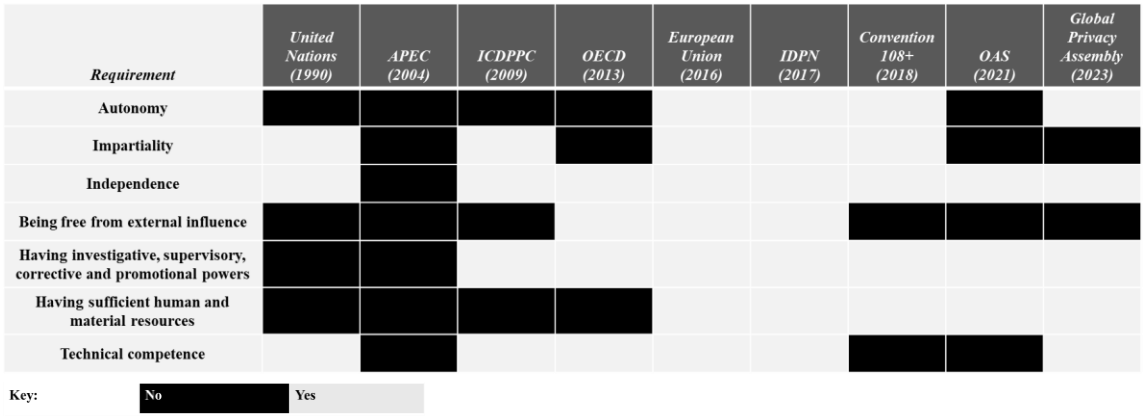
Fourth: as illustrated in the table below, in its resolution 45/95 the General Assembly does not mention the following options for conducting international data transfers: use of contractual clauses, binding corporate rules, certification mechanisms, authorization by the supervisory authority, authorization by the data subject, and international treaties.

Table 4
Options for conducting international transfers of personal data explicitly mentioned in international documents



Fifth: as can be verified in the table below, in its resolution 45/95 the General Assembly does not mention the following requirements that must be met or characteristics that must be possessed by supervisory or personal data protection authorities: autonomy, being free from external influence, having investigative, supervisory, corrective and promotional powers, and having sufficient human and material resources to perform their functions.

Table 5
Requirements for supervisory or personal data protection authorities explicitly mentioned in international documents



In view of the results of this analysis, the proposed updated text incorporates the topics not currently addressed in General Assembly resolution 45/95, in order to ensure that it is complete and sufficient to respond to current needs, so as to enable the proper processing of personal data.

In the light of the foregoing, it is proposed that the General Assembly of the United Nations adopt the following text amending its resolution 45/95 of 14 December 1990:

Proposal to amend United Nations General Assembly resolution 45/95 of 14 December 1990

Guidelines for the processing of personal data

The procedures for implementing regulations concerning the processing of personal data are left to the initiative of each State, subject to the following orientations:

A. Principles concerning the minimum guarantees that should be provided in national law to ensure the proper processing of personal data

1. Principle of lawfulness and fairness

The collection, use, circulation and processing of personal data, and any other activity involving personal data, must be carried out in accordance with the laws of each country and for lawful purposes.

Information about persons (personal data) must not be collected or processed in unfair, deceptive, unlawful or fraudulent ways, nor should it be used for ends contrary to human dignity or to the purposes and principles of the Charter of the United Nations.

2. Principle of data accuracy or quality

Personal data must be reliable, complete, accurate, timely, verifiable and relevant to the purpose of the processing, and they must be updated whenever necessary, either unprompted – by the controller or processor – or at the request of the data subject. Data that are partial, incomplete, fractured or misleading must not be processed.

Controllers and processors of personal data must take measures to ensure the quality, timeliness, completeness, accuracy and relevance of the data.

3. Principle of purpose specification, necessity, proportionality and temporariness

Data must be processed only for specific, explicit and legitimate purposes and must not later be processed in a manner incompatible with those purposes. Only data that are necessary, relevant and appropriate for the purposes of the processing should be processed. Data must be limited and must not be excessive for the purpose for which they were collected.

The purpose of the processing of personal data must be specified, legitimate and, when the data are collected, receive a certain amount of publicity or be brought to the attention of the person concerned (the data subject), in order to make it possible subsequently to ensure that: (a) all the personal data collected, recorded or processed remain relevant and adequate for the purposes so specified; (b) none of the said personal data is used or disclosed without the consent of the person concerned or for purposes incompatible with those specified; (c) the period for which the personal data are kept does not exceed that which would enable the achievement of the authorized or permissible purpose of their processing.

Personal data must be kept only for as long as necessary to fulfil the purposes for which they are collected or processed and must be deleted or anonymized when they are no longer needed for those purposes.

4. Principle of interested person (data subject) access

Everyone who offers proof of identity has the right to know whether information concerning him or her is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressees. Provision should be made for a remedy, if need be, with the authority responsible for ensuring respect for these principles. The cost of any rectification should be borne by the controller or processor of the personal data. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence.

5. Principle of non-discrimination and non-manipulation

Subject to cases of exceptions restrictively envisaged under principle 6, data likely to give rise to unlawful or arbitrary discrimination, including information on an individual’s racial or ethnic origin, religious, philosophical or other beliefs, membership in an association or trade union, social or human rights organization or organization that promotes the interests of any political party or that safeguards the rights of opposition parties, as well as data relating to health, sexual life and sexual preferences, genetic or biometric data intended to uniquely identify a natural person, and also neural data, must not be recorded.

The processing of neural data, or neurodata, must not be used to manipulate or alter the freedom of thought and consciousness of an individual, making him or her dependent on a third party or altering his or her ideas, security or independence or his or her natural cerebral identity or neurocognitive integrity. Nor may such data be processed for purposes other than the promotion of health and the diagnosis, rehabilitation and alleviation of disease in the context of the right to health, or scientific research in the fields of biology, psychology and medicine aimed at alleviating suffering or improving health.

6. Power to make exceptions

Departures from principles 1 to 4 may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others, especially persons being persecuted (humanitarian clause), provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards.

Exceptions to principle 5 relating to the prohibition of discrimination, in addition to being subject to the same safeguards as those prescribed for exceptions to principles 1 and 4, may be authorized only within the limits prescribed by the Universal Declaration of Human Rights and the other relevant instruments in the field of protection of human rights and the prevention of discrimination.

7. Principle of security

Appropriate, reasonable, sufficient, useful and timely preventive measures must be taken to protect files, databases and information systems against both natural dangers, such as accidental loss or destruction, and human dangers, such as unauthorized access, fraudulent misuse of data, contamination by computer viruses, and the manipulation, loss, modification, destruction, damage, disclosure or other misuse of information.

Security measures concerning the processing of personal data must be regularly audited, reviewed and maintained and continuously updated.

Measures to ensure the adequate and timely management of potential security incidents must also be taken, in order to prevent harm to data subjects, controllers, processors and society at large.

8. Principle of confidentiality

All persons involved in the processing of personal data that are not public in nature have an obligation to ensure the confidentiality of the information, even after the end of their relationship with any activities involved in the processing of the data, and may only supply or communicate personal data as part of the implementation of activities authorized by law or by the data subject.

9. Enhanced protection for sensitive data

Some data are sensitive and affect the privacy of the data subject or, if used improperly, may lead to discrimination against the data subject. Such data include those that reveal the data subject’s racial or ethnic origin, political leanings, religious or philosophical beliefs or membership in a trade union, social or human rights organization or organization that promotes the interests of any political party or that upholds the rights and guarantees of opposition parties, as well as data relating to health, sexual life and sexual preferences, neurodata (neural data), and genetic or biometric data intended to uniquely identify a natural person.

This sensitive information must be subject to special enhanced responsibility measures with regard to security, confidentiality, access and restrictions on circulation, in order to prevent such data from being accessed, improperly used, manipulated or destroyed.

10. Special protection for data relating to children and adolescents

When processing personal data relating to children and adolescents, the priority shall be the protection of their best interests, in accordance with the Convention

on the Rights of the Child and other international instruments aimed at ensuring the well-being and comprehensive protection of children and adolescents.

The academic education of children and adolescents shall include the promotion of the responsible, appropriate and safe use of technology, awareness-raising regarding the possible risks faced in digital environments with regard to the improper processing of personal data, and the fostering of respect for their freedoms and rights, and the rights of others.

The personal data of children and adolescents must be subject to special enhanced responsibility measures with regard to security, confidentiality, access and restrictions on circulation, in order to prevent such data from being accessed, improperly used, manipulated or destroyed.

11. Principle on automated individual decisions

The data subject shall have the right not to be subject to decisions that produce legal effects for or significantly affect him or her that are based solely on automated processing intended to evaluate, without human intervention, certain personal aspects of the data subject or to analyse or predict, in particular, his or her professional performance, economic situation, state of health, sexual preferences, reliability or behaviour.

The foregoing shall not apply when the automated processing of personal data is necessary for the conclusion or performance of a contract between the data subject and the data controller, is authorized by the domestic law of States, or is based on the demonstrable consent of the data subject.

However, when it is necessary for the contractual relationship or the data subject has given consent, the data subject shall be entitled to obtain human intervention, receive an explanation of the decision taken, express his or her point of view and challenge the decision.

12. Principle of transparency

Before or at the time the data are collected, the identity and contact details of the data controller, the specific purposes for which the personal data will be processed, the legal basis for the processing, the recipients or categories of recipients to whom the personal data will be communicated, the information to be transmitted and the rights of the data subject in relation to the personal data to be collected must be specified. When data processing is based on consent, personal data must be collected only with the prior, unambiguous, free and informed consent of the data subject.

If the data subject is the object of automated decision-making, profiling, or decision-making processes involving artificial intelligence or other technologies, he or she must be informed, in a clear and simple manner, about the following:

- The processes involving automation, artificial intelligence or any other technology that will be used in the processing of the data.
- The reasoning behind a decision that affects him or her, through clear, truthful and meaningful information, so that he or she can understand the basic elements of the decision-making based on his or her personal data.
- The information that will be used to make the decision.
- Whether or not the quality of the decision was verified through qualified human oversight.
- Additional information that would enable the data subject to understand how automated decisions might positively or negatively affect him or her.

The information must be provided in clear, simple and easily understood language.

13. Principle of explainability

When requested by the data subject, the data controller or data processor must provide explanations in clear and understandable language regarding the information and the process used to make a decision affecting the data subject.

These explanations must not only accurately reflect the reasoning of the system used to make the decision, but must also be comprehensible, truthful, complete, easily understood and specific or directly related to the case of the affected data subject. All information and explanations necessary for people to understand how decisions that affect them were made and to have the tools to defend their human rights or request a review of a decision must be provided.

Furthermore, there must be an accountable human being with whom concerns related to automated decisions can be raised and rights can be exercised, and who can also trigger evaluation and review of the automated decision-making process.

14. Principle of demonstrated or proactive responsibility (accountability)

Data controllers and processors must adopt and implement useful, timely, appropriate and effective technical, organizational and other measures to ensure and demonstrate that processing is being carried out in accordance with the principles set out in the present resolution.

These measures must be audited and updated periodically to ensure that they are functioning properly, measure the degree to which the rights of data subjects are protected and assess compliance with these principles.

15. Data processing impact assessments

Where a type of processing, in particular one using new technologies, by virtue of its nature, scope, context or purposes, is likely to entail a high risk to the rights and freedoms of natural persons, the data controller shall, prior to the processing, carry out an assessment of the potential impact of processing operations on the protection of personal data, with a view to taking preventive measures to address and mitigate the risks identified.

An impact assessment must be carried out, inter alia, when personal aspects relating to natural persons are to be systematically and extensively evaluated on the basis of processing that is automated, including profiling, and that forms the basis for decisions that produce legal effects for the natural person or similarly significantly affect the natural person; or when massive or large-scale processing of data that is sensitive or relates to minors is planned.

16. Privacy by design and by default

Taking reasonable account of the costs of implementation of the processing, the state of the art, the nature, circumstances and purposes of the processing, as well as the likely risk and the severity thereof, the data controller (and potentially the data processor) must implement appropriate technical and organizational measures to ensure that the principles set forth in the present resolution are given effect when determining the applicable means of processing and during the processing itself.

Furthermore, those measures must be applied with a view to ensuring that, by default, only personal data that are necessary for each specific purpose of the processing are processed. This obligation applies also to the amount of data to

be processed, the extent of the processing, the data storage period and the accessibility of the data.

17. Precautionary principle

If there is a lack of certainty regarding the potential harm to the data subject or to society that may result from the processing of personal data, the data controller or data processor must, in order to avoid causing serious and irreversible harm, refrain from carrying out the processing or take precautionary or preventive measures to protect the rights of the data subject, his or her human dignity and other human rights.

The precautionary principle also applies when the risks or the extent of the harm that would or might result are not known in advance because there is no way of determining the effects that the data processing would have in the medium or long term.

18. Principle of favourable or prevailing interpretation

In case of doubt regarding the interpretation and application of these principles, the interpretation most favourable to the data subject shall prevail.

19. Principle of self-regulation

The data controller may, on a voluntary basis, join binding self-regulation schemes that are aimed at, inter alia, contributing to the proper application of the present principles and establishing procedures for resolving conflicts between data controllers and data subjects, without prejudice to other mechanisms that may be established by the applicable national law on the matter, taking into account the specific characteristics of the personal data processing, as well as the effective exercise of and respect for the rights of the data subject.

For the purposes of the preceding paragraph, codes of ethics and certification systems with their respective trust seals may be developed to contribute to the achievement of the objectives set forth in this article.

20. Principle of effective protection of the rights of subjects of personal data

Useful, effective, simple and expeditious mechanisms shall be adopted to guarantee that subjects of personal data have the right to the following: access, rectification, deletion (erasure), objection, portability, not be the object of automated decision-making that produces legal effects for or significantly affects them, and compensation for damage suffered by them as a result of improper processing of their information.

In addition to the judicial or administrative actions provided for in national regulations, the use of alternative dispute resolution methods for disputes concerning the processing of personal data shall be promoted.

21. Supervision and sanctions

Each State must designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth in the present resolution. This authority must offer guarantees of impartiality, independence vis-à-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties must be envisaged, together with the appropriate individual remedies.

The authority shall have full autonomy and shall not be subject to any external influence, direct or indirect, and it shall not request or accept any order or

instruction. Its staff shall have experience and specialized knowledge regarding the processing of personal data.

The authority shall be designated through a transparent public procedure, for a specified period of time. The individuals so designated may not be removed, except for serious reasons previously established in the respective regulations of each country.

The authority must have sufficient investigative, supervisory, decision-making, promotion, sanctioning and other powers as may be necessary to guarantee the rights of data subjects and the proper processing of their information. It must also have sufficient economic, human and technological resources to perform its functions properly and in a timely manner.

22. Transborder data flows

When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the proper processing of personal data, information should be able to circulate as freely as inside each of the territories concerned.

If there are insufficient safeguards, limitations on such circulation may not be imposed unduly and only insofar as the protection of human rights demands.

In order to determine whether a country has comparable safeguards, the following elements, inter alia, may be assessed:

(a) The rule of law; respect for human rights and fundamental freedoms; and the relevant laws, both general and sectoral, on the processing of personal data;

(b) The existence and effective functioning of one or more independent supervisory authorities responsible for ensuring and enforcing compliance with data protection rules, having adequate enforcement powers as well as powers to assist and advise data subjects and cooperate with data protection authorities;

(c) International commitments undertaken by the third country or international organization concerned, or other obligations arising from legally binding agreements or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

The data controller and data processor may conduct international transfers of personal data in any of the following cases:

- It has been proven that the country or part of its territory, the sector, the activity or international organization to which the personal data are to be exported has guarantees for ensuring the proper processing of the personal data that are comparable to those provided for in the national laws of the country from which the data are to be exported.
- The exporter and recipient enter into a contract or any other legal instrument that provides sufficient guarantees and sets out the scope of the processing of personal data, the obligations and responsibilities assumed by the parties and the rights of the data subjects. The supervisory authority may validate contracts or legal instruments, as provided for under national law.
- The exporter and the recipient adopt a binding self-regulation scheme or a certification mechanism approved by the data authority of the country from which the personal data are to be sent.

- The data subject or the supervisory authority of the country of the exporter authorizes the transfer, in accordance with the applicable national laws.

States may authorize other exceptions through international laws or instruments.

23. International collection of personal data

States shall adopt appropriate, useful and timely measures to ensure the proper processing of personal data and the effective protection of the rights of individuals whose information is collected by data controllers or data processors which are located in countries other than the country of domicile or residence of the subject of the personal data and which have no physical headquarters or establishment in the country of domicile or residence of the subject of the personal data (international data collector).

In addition, States shall cooperate with one another, with data protection authorities and with data subjects to ensure the achievement of the objective set forth in the preceding paragraph.

The fact that the international data collector is not present in and does not have a physical headquarters or establishment in the country of the data subject should not generate or facilitate impunity or a lack of protection of the rights of individuals.

24. Field of application

The present principles shall be made applicable, in the first instance, to all public and private processing of personal data, regardless of the means or technologies used for the processing.

B. Application of the guidelines to the processing of personal data by governmental international organizations

Governmental international organizations shall apply the present guidelines to the processing of personal data, subject to any adjustments that may be required to take account of any differences that might exist between files or information systems for internal purposes, such as those that concern personnel management, and files or information systems for external purposes concerning third parties having relations with the organization.

Each organization shall designate the authority that, under its statute, is competent to supervise the observance of these guidelines.

Humanitarian clause

States shall adopt special measures on the processing of personal data to facilitate and support humanitarian action aimed at protecting and assisting vulnerable persons in the context of armed conflict, violence, emergency situations or natural disasters.