Gap Analysis

The Senegalese Data Protection Law and the General Data Protection Regulation

This document was commissioned under contract for a gap analysis of the Senegalese Data Protection Law and the General Data Protection Regulation by the Norwegian Red Cross (NorCross). The document was prepared by Lina Jasmontaite and Julia Zomignani Barboza under the supervision of Paul Quinn. The document can be made available for transparency and information purposes only and does not constitute legal advice.

Table of Contents

1. Introduction

Senegal can be seen as a success story when it comes to addressing risks associated with the processing of personal data. While the Senegalese legal framework governing data protection is relatively new (dating from 2008), the national data protection authority (La Commission de protection de données personnelles – CDP) has been active in promoting compliance with the national data protection law through public awareness campaigns. Furthermore, the CDP has power to investigate and issue fines for data mishandling (i.e., data security breaches). Although to date no major fines have been issued for mishandling personal data, there is no doubt regarding the CDP's proactiveness, as numerous companies have been presented with notices requiring them to adjust their business practices concerning the handling of personal data.[1] Despite such proactiveness, in the past, Privacy International (a UK-based charity that promotes the right to privacy, including by advocating for strong privacy laws) expressed concerns that due to the lack of an operational budget set out by the state, CDP's activities were rather limited and even ceased in 2013.[2] However, in recent years, the CDP has increasingly been involved in multiple initiatives, both nationally and internationally.[3] For example, the CPD is an active member of the Association francophone des autorités de protection des données personnelles (AFAPDP), and, as such, hosted the12th AFAPDP annual conference in September 2019.

Against this background, the following sections will provide a comparative analysis between the General Data Protection Regulation (EU) 2016/679 (GDPR), increasingly considered as the 'gold standard' for the protection of personal data, and the Senegalese Data Protection Law.

2. Regulatory framework

The Senegalese legal framework for the processing of personal data is comprised of the Data Protection Act (Law 2008-12, January 25 2008); the Decree on the Application of the Data Protection Act (2008-721, June 30 2008); and the Cybercrime Law (Law 2008-10, January 25 2008). The two laws further substantiate Articles 13 and 16 of the Senegalese Constitution which provide protection of informational and physical privacy.[4]

---

[1] For more details see: https://www.cdp.sn/sanctions.

[2] See: Privacy International, Privacy International submits stakeholder reports to Human Rights Council on the right to privacy in China, Senegal and Mexico, July 2013, available https://privacyinternational.org/blog/1275/privacy-international-submits-stakeholder-reports-human-rights-council-right-privacy.

[3] Victor Ndonnang and Robin Wilton, Senegal First African Country to Implement Recommendations of 'Personal Data Protection Guidelines for Africa', October 2018, available: https://www.internetsociety.org/blog/2018/10/senegal-first-african-country-to-implement-personal-data-protection-guidelines-for-africa-recommendations/

[4] Note, while the Senegalese Constitution considers the domicile to be inviolable, exceptions to this rule of the thumb can be made in situations where it is necessary to protect the public order against imminent threats [menaces], singularly to combat the risks of epidemic or to protect youth in danger.

In 2016, the revision of procedural and substantive provisions of the criminal codes included data mishandling as a criminal offence that incurs in criminal sanctions.[5] Legal persons can now be held accountable for offences concerning data theft, fraud, extortion of funds and blackmail involving computer data.[6]

There is no sector specific regulation concerning the processing of personal data, so it can be suggested that the Senegalese data protection law provides an overarching protection that regulates all sectors.

Senegal is not a unique country within Africa when it comes to the protection of personal data, as other 23 African countries (e.g., Angola, Benin, Burkina Faso, Chad, Equatorial Guinea, Mali, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Malawi, Morocco, Niger, Kenya, South Africa, Tunisia, Zambia) have adopted data protection and privacy laws.[7] As concerns over processing of personal data are being widely recognised, in particular issues concerning special categories of data revealing health status, political and religious views,[8] many other countries are also on the path to enact data protection laws, such as Nigeria, Togo, Tanzania, Uganda and Zimbabwe.

3. International commitments

Senegal has signed and ratified almost all of the United Nations core human rights instruments. As part of its human rights commitments, Senegal must provide measures to ensure that Article 12 of the Universal Declaration of Human Rights (UDHR)[9] and Article 17 the International Covenant on Civil and Political Rights (ICCPR), which prescribe the right to freedom from arbitrary interference with privacy, family, home or correspondence. Besides human rights commitments in general, in August 2016, Senegal has undertaken two major international commitments concerning specifically the processing of personal data and information security:

- Firstly, Senegal ratified the African Union (AU) Convention on Cyber Security and Personal Data Protection, which was adopted on 27 June 2014 with support of a group

[5] Loi n° 2016-30 du 08 novembre 2016 modifiant la loi n° 65-61 du 21 juillet 1965 portant Code de procédure pénale et loi n° 2016-29 du 08 novembre 2016 modifiant la loi n° 65-60 du 21 juillet 1965 portant Code pénal.

[6] Add provisions from the criminal codes.

[7] Based on Privacy International, '2020 is a crucial year to fight for data protection in Africa' < https://privacyinternational.org/long-read/3390/2020-crucial-year-fight-data-protection-africa> and Consumers International, 'The State of Data Protection Rules around the World: A Briefing for Consumer Organisations' 3 <https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf>.

[8] Privacy International, '2020 is a crucial year to fight for data protection in Africa' < https://privacyinternational.org/long-read/3390/2020-crucial-year-fight-data-protection-africa>.

[9] The UDHR is a non-binding declaration and therefore there are no mechanisms to ensure its enforcement.

of 54 African states. This means that provisions of the Convention now constitute an integral part of the applicable framework to the protection of personal data.

- Secondly, Senegal signed the Council of Europe Convention (CoE) for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108), which entered into force in December 2016. Convention No.108 (which is open for signature by the non-member States of the CoE) was adopted in 1981 and it is the first binding international instrument which is concerned with the protection of individuals against abusive personal data practices. It is often suggested that this Convention paved the way for the EU Data protection Directive 95/46/EC (which preceded the GDPR). Senegal has ratified this Convention without reservations, and it could be argued that in this way it demonstrated the ambition to uphold a high data protection standard within its jurisdiction.

When considering the status of international treaties in Senegal, it should be noted that Article 79 of the Constitution of Senegal stipulates that international law takes precedence over domestic law. Consequently, this means that international human rights instruments are part of the domestic law of Senegal and take precedence over any state measure.[10]

4. Is the Senegalese data protection framework "adequate" for the EU standards?

It is suggested that the Senegalese legislature, when drafting the country's data protection legislation, drew inspiration from the EU Data Protection Directive 95/46/EC (the GDPR's predecessor) as one of the leading instruments in the field at the time.[11] However, thus far, Senegal has not been awarded an adequacy decision by the European Commission that would allow free data flows between the EU and Senegal.

The Court of Justice of European Union (CJEU) in Case C-362/14 Maximillian Schrems v Data Protection Commissioner reasoned that the 'adequate level of protection' must be understood as requiring the third country to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46/EC.[12] To the best of our knowledge, there are no recorded reasons why such procedure has never been initiated for Senegal or other African countries that have enacted data protection laws resembling the provisions of the EU Data Protection Directive 95/46/EC. However, the absence

[10] Boshe P. (2016) Protection of Personal Data in Senegal. In: Makulilo A. (eds) African Data Privacy Laws. Law, Governance and Technology Series, vol 33. Springer, 264.
[11] Ibid 259-275.
[12] Case C-362/14 Maximillian Schrems v Data, paragraph 73.

of an adequacy decision means that even though some of the provisions and definitions may appear similar or close in their meaning and scope under both frameworks, the Senegalese data protection framework cannot be assumed to ensure the same level of protection to data subjects' rights to privacy and the protection of their personal data as the European Union. Consequently, certain safeguards need to be taken to enable data transfers between the EU and Senegal. The concept of such safeguards was introduced in Article 26.2 of Directive 95/46/EC and it was further clarified in Article 46 of the GDPR, which repealed the Directive. Such appropriate safeguards may include:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules

(c) standard data protection clauses adopted by the Commission;

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission;

(e) an approved code of conduct; or

(f) an approved certification mechanism.

With the GDPR repealing the Data Protection Directive, requirements for adequacy decisions have been further detailed in Article 45, taking into account the reasoning of the CJEU in the abovementioned Case C-362/14 Maximillian Schrems v Data Protection Commissioner. Currently, for an adequacy decision to be issued, the European Commission must assess the following elements in the concerned country:

- the rule of law;
- respect for human rights and fundamental freedoms;
- relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and
- the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures,
- including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation,
- case-law;
- effective and enforceable data subject rights and effective administrative;
- judicial redress for the data subjects whose personal data are being transferred;
- the existence and effective functioning of an independent supervisory authority in the third country; and

- the international commitments the third country has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

While the framework of Article 45 can be considered to be a good practice to follow that would allow a thorough understanding of the Senegalese data protection framework, many of its crucial aspects fall outside the scope of this gap analysis (e.g., analysis of the rule of law). In order to perform the gap analysis between the two frameworks the following will be analysed:

- key concepts concerning the protection of personal data;
- grounds for lawful and fair processing of personal data;
- the purpose limitation principle;
- the data quality and proportionality principles
- limited data retention principle;
- the security and confidentiality principles;
- the transparency principle;
- the rights of access, rectification, erasure and objection; and
- restrictions on international data transfers.

5. Key data protection concepts

In this section we outline key definitions provided in the Senegalese data protection law (on the left column of the table below). All of these definitions, apart from the concept of data breach, are listed in Article 4 of that law. For comparison, we also include their 'counterpart' definition from the GDPR (on the right column). In order to match definitions provided in the two regulatory tools we used the list of terms prepared by the French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés – CNIL).[13] At the end of this section, we provide a list of key GDPR concepts that are not defined in the current Senegalese data protection law.

Senegalese data protection law[14]	GDPR
Code of conduct: any draft rules, including user charters, developed by the responsible for	The GDPR does not define the term 'code of conduct', however, it encourages the use of codes

[13] CNIL, Lexique français anglais sur la protection des données, available: https://www.cnil.fr/fr/lexique-francais-anglais-sur-la-protection-des-donnees.

[14] LOI n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel, available: https://www.cdp.sn/content/loi-n%C2%B0-2008-12-du-25-janvier-2008-portant-sur-la-protection-des-donn%C3%A9es-%C3%A0-caract%C3%A8re

processing, in accordance with this Law, in order to establish correct use of computing resources, the Internet and electronic communications of the concerned and approved by the Commission for Personal Data.	of conducts. Codes of conduct foreseen in Article 40 of the GDPR are meant to include best practice to follow concerning the processing of personal data in a specific sector or business for both controllers and processors.
Electronic communications: transmissions, or receptions of signs, signals, writings, images or sounds, electronically or magnetically.	The GDPR does not define the term 'electronic communications'. Directive 2002/58/EC (ePrivacy Directive) is *lex specialis* particularising the provisions of the GDPR with respect to the processing of personal data in the electronic communication sector.
Temporary copies: data temporarily copied to a dedicated space, for a limited time, for the purposes of operating the processing software.	The GDPR does not define temporary copies.
Consent of the person concerned: any expression of intent, unequivocal, free, specific and informed by which the person is subject to manual or electronic processing.	**Consent** of the data subject means the freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Addressee of the processing of personal data (i.e., data recipient): any person authorised to receive such data other than the data subject, the person in charge of the subcontractor and those persons who, by reason of their duties, are responsible for processing data. However, the public authorities legally empowered, within the framework of a particular mission or the exercise of a right of communication, may request the data controller to communicate personal data to them.	**Recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
Personal data: any information relating to a natural person identified or identifiable directly or indirectly by reference to an identification number or to one or more elements, specific to its physical, physiological, genetic, psychic, cultural, social or economic characteristics.	**Personal data** means any information relating to an identified or identifiable natural person ('data subject');
The concerned person (i.e., data subject) any natural person who is the subject to the processing of personal data.	**Data subject** is a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Genetic data: any data concerning the hereditary characteristics of an individual or a group of related individuals.	**Genetic data** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Sensitive data: all personal data relating to opinions or religious, philosophical, political, union, sexual or racial activities; health; social measures; prosecutions, penal or administrative sanctions.	**Special categories of data** include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. As a general rule, the processing of such type of data shall be prohibited. All exceptions to this rule are provided for in Article 9 of the GDPR.
Data in the field of health: any information concerning the physical state and mental health of a data subject, including the abovementioned genetic data.	**Data concerning health** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
Personal data file: any structured set of accessible data according to certain criteria, whether this group is centralised, decentralised or distributed in any functional or geographical way.	**Filing system** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
Interconnection of personal data: any connection mechanism consisting of the linking of data processed for a specific purpose with other data processed for the same or different purposes, or linked by one or more processing operations.	**Profiling** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Third country: any State other than Senegal.	The GDPR does not define the term 'third country.' Its understanding within the EU law is stemming from Article 2(5) of the Regulation (EU) 2016/399, which foresees that a third country is a country that is not a member of the European Union as well as a country or territory whose citizens do not enjoy the European Union right to free movement.
Person concerned (i.e., data subject): any natural person who is the subject of data processing of his or her own personal attributes.	**Data subject** is a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Direct prospecting: any solicitation carried out by means of sending a message, which supports or has the particular commercial, political or charitable nature intended to promote, directly or indirectly, goods, services or the image of a person selling goods or providing services.	The GDPR does not define the term 'direct marketing', however, it foresees in Article 21.2 that 'where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such

	marketing, which includes profiling to the extent that it is related to such direct marketing'.
Responsible for the processing (i.e., controller): the natural or legal person, public or private, or another organisation or association which, alone or jointly with others, makes the decision to collect and process personal data and determine the purposes thereof.	**Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data processor: any natural or legal person, public or private, or any other organisation or association that processes data on behalf of the controller.	**Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Online service: any added-value service delivery based on telecommunications and / or information technology, aimed at giving a natural or legal person, public or private, the possibility of carrying out activities, procedures or formalities, etc. interactively and at a distance.	**Information society service** entails any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.
Third party: any natural or legal person, public or private, or any other organisation or association other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or sub-administrator, are entitled to process the data.	**Third party** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
Processing of personal data: any transaction or set of transactions provided for in Article 2 of the law,[15] whether or not using automated processes, and applied to data, such as collection, exploitation, registration, organisation, conservation, adaptation, modification, extraction, safeguarding, copy, consultation, use, communication by transmission, dissemination or any other form of provision, reconciliation or interconnection, and the locking, encryption, deletion or destruction of personal data.	**Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Apart from the numerous definitions that are set forth in the Senegalese data protection framework, some key concepts from the GDPR are missing. These include:

- **biometric data**, which 'means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a

[15] Article 2 defines the scope the law. It foresees that the law applies to all processing in the Senegalese territory (or in a place where Senegalese laws apply), and to processing established by a data controller outside of Senegal, regardless of its legal form, if using processing equipment in the territory of Senegal (except for transit purpose equipment).

natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data';[16]

- **personal data breach** 'means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed';[17]
- **profiling,** which entails 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;'[18] and
- **pseudonymisation**, which 'means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.'[19]

6. Lawful and fair processing

Article 34 of the Senegal Data Protection act requires that personal data are processed in a lawful, fair and not fraudulent way. Article 33 stipulates that, apart from consent, the processing of personal data can be conducted if it is necessary for:

1) the compliance with a legal obligation of the controller;

2) the performance of a public interest[20] or the exercise of official authority vested in the controller or the third party to whom the data are communicated;

3) the performance of a contract to which the data subject is a party or the preparation of contractual obligations; and

4) safeguarding the interest or fundamental rights and freedoms of the data subject.

Considering this legal set-up, it could be suggested that the grounds for processing data in the Senegalese framework are similar to the EU ones, albeit the EU framework is to some extent

[16] Article 4 (14), GDPR.
[17] Article 4 (12), GDPR.
[18] Article 4 (4), GDPR.
[19] Article 4 (5), GDPR.
[20] It is important to note that acting in the public interest is not suffice. A controller must be carrying out a specific task in the public interest which is laid down by law or exercising official authority (for example, a public body's tasks, functions, duties or powers) which is laid down by law.

more nuanced and specific. For example, GDPR foresees that the processing of personal data may be lawful if it 'is necessary in order to protect the vital interests of the data subject or of another natural person.'[21] At the same time, the EU approach provides some discretion to data controllers (who are not public authorities) to conduct business and it allows processing for 'the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.'[22]

7. The purpose limitation principle

In essence, the purpose limitation principle protects data subjects by setting limits on how data controllers are able to use their data while also offering some degree of flexibility for data controllers. To attain this aim, the concept of purpose limitation has two main building blocks: i) personal data must be collected for "*specified, explicit and legitimate*" purposes (i.e., purpose specification) and ii) not be "*further processed in a way incompatible*" with those purposes (i.e., compatible use).

Following this principle, as explained by the European Regulators in the set-up of the Article 29 Working Party (WP29),[23] "the *purposes of the data collection"*

- must be defined prior to the collection (i.e., companies should be able to predict the data uses before collecting data);
- clearly communicated in an intelligible and transparent form to data subjects; and
- be legitimate and fall under one of the legal grounds listed in section 6 (e.g., consent, performance of a contract, etc.).[24]

In the online context, the WP29 recommends using layered notices as such notices would allow data subjects – users – to select the level of detail they would like to get concerning the processing operation. Needless to say, a vague and generic language should be avoided when defining the purposes of the processing.

The Senegalese data protection law includes the purpose limitation principle in Article 35. According to this Article, personal data must be collected for a specified, explicit and legitimate purpose(s), and cannot be processed in a way that is incompatible with that purpose(s).

[21] Article 6.1(d), GDPR.
[22] Article 6.1(f), GDPR.
[23] The Article 29 Working Party was the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018 (entry into application of the GDPR), from then onwards this body was replaced by the European Data Protection Board. The Article Working Party 29 opinions and guidance documents remain relevant, where consistent with the new legal framework.
[24] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, WP 203.

Additionally, any additional purpose (or further processing) must also be adequate, relevant and not excessive in relation to the initial purpose of data collection.

8. Data quality and proportionality principles

As a rule, data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (the so-called data minimisation principle). Additionally, personal data should be accurate and where necessary kept up to date.

Like the EU approach, the Senegalese data protection law includes the data quality principle. Following Article 36 of the Senegalese data protection law, the collected data must be accurate and, if necessary, updated. Any measure must be taken to ensure that inaccurate or incomplete data, in the light of the purposes for which they are collected and subsequently processed, are deleted or rectified.

At this point, it should be noted that the principle of proportionality, which is at the core of data protection law,

is applicable throughout the data Processing cycle and may be invoked at different stages of data processing operations. It requires consideration of whether a particular action or measure related to the processing of personal data is appropriate to its pursued aim (e.g. is the selected legitimate basis proportionate to the aim pursued? Are technical and organizational measures proportionate to the risks associated with the Processing?).[25]

9. Data retention

Data should be kept for no longer than necessary. Article 35 of the Senegalese data protection law stipulates that personal data must be kept for a period not exceeding the period necessary to achieve the purposes for which they were collected or processed. Beyond this required period, the data can only be stored if specifically processed for historical, statistical or research purposes prescribed by law.

10.Security and confidentiality principles

The Senegalese data protection law in Article 38 foresees that personal information must be kept confidential and secure. Article 70 elaborates on confidentiality measures to be taken by controllers and it requires them to have a contract in place in situations where the processing is entrusted to a processor. The specific security measures are foreseen in Article 71 of the same

[25] Christopher Kuner and Massimo Marelli, 'Handbook on Data Protection in Humanitarian Action' 164, 26.

law, according to which, the controller is required to take every precaution with regard to the nature of data and, in particular, to prevent them from being distorted (altered), damaged (destroyed), or accessed by unauthorised third parties. In particular, the controller should take measures aiming:

(1) to ensure that, for the use of an automated data processing system, the authorised persons can only access personal data within their competence (i.e., on a need-to-know basis);

(2) to verify the identity of third parties by whom personal data can be processed;

(3) to guarantee that the identity of the persons who have access to the information system is known and to record what data has been read or entered into the system, when and by whom;[26]

4) to prevent unauthorised persons from gaining access to the premises and equipment used for data processing;

5) to prevent data files from being read, copied, modified, destroyed or displaced by an unauthorised person;

6) to prevent the unauthorised entry of any data into the information system as well as any unauthorised access, modification or deletion of recorded data;

7) to prevent data processing systems from being used by unauthorised persons through data transmission facilities;

8) to prevent the communication of data and the transport of data, as well as that the data may be read, copied, modified or deleted in an unauthorised manner;

9) to back up the data by making backup copies;

10) to refresh and, if necessary, convert the data for a long-term storage.

11. Obligation to obtain sufficient guarantees

Furthermore, the data controllers must require processors to guarantee that the security measures they take are sufficient to secure the data (Article 39 of the Senegalese data protection law). The processor must follow the instructions of the data controller.

12. Transparency

According to WP29, transparency has been regarded as the EU solution to tackle a well-established and documented information asymmetry between controllers and data subjects,

[26] The GDPR does not explicitly require logging but it is considered to be a key tool providing accountability. It allows to monitor and audit internal processing within any automated processing systems, and to know which third parties were enabled to have access to data. In addition, logging enables controllers and processors to monitor systems for inappropriate access and/or disclosure of data, to verify the lawfulness of any processing, and to ensure the integrity and security of personal data.

which results in the lack of data subjects' control over the processing of their personal data.[27] Therefore, the introduction of a general transparency principle in the GDPR was perceived as an important step strengthening data subjects' rights.[28]

While information notification obligations concerning the processing[29] have been primarily considered to be the embodiment of the transparency principle, such approach entailed limitations that were identified by the regulators. In particular, WP29 argued that transparency should extend to the data subject's right to access one's data by allowing to obtain 'not just on the basic or primary data, but also on the derived or consolidated information.'[30] Furthermore, WP29 was of the opinion that the GDPR 'should provide alternative solutions in order to enhance transparency.'[31]

In a similar vein, the transparency principle is of a crucial importance to the Senegalese data protection law. Article 37 foresees that the principle of transparency requires controllers to keep all relevant parties informed about its activities. This requirement also entails an obligation to provide data subjects with information concerning the processing, including the possibility to exercise their data subjects' rights.

13. Rights of data subjects

Rights of data subjects gained fresh prominence with the revision of the EU data protection framework[32] as a result of the regulatory expansion and further articulation of this topic as well as the addition of a new right to data portability. In order to refer to all of the rights at once, the term 'control rights' is sometimes used.[33] The term also corresponds with the idea presented in

[27] For example, Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things (WP223, 2014); Opinion 02/2013 on apps on smart devices (WP202, 2013); Opinion 05/2012 on Cloud Computing (WP196, 2012)

[28] Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals (WP191, 2012) 4.

[29] Also, referred to as an information notice.

[30] Article 29 Data Protection Working Party, 'Privacy on the Internet. An Integrated EU Approach to On-Line Data Protection' (2000) 71 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37en.pdf>.

[31] Article 29 Data Protection Working Party and Working Party on Police and Justice, 'The Future of Privacy Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data' (2009) WP 168 3.

[32] With the GDPR repealing Directive 95/46/EC.

[33] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015); Claudia Quelle, 'Not Just User Control in the General Data Protection Regulation. On the Problems with Choice and Paternalism, and on the Point of Data Protection', *IFIP AICT 498 (2017)* (2017) <https://www.ssrn.com/abstract=2925410>.

the GDPR – '[N]atural persons should have control of their own personal data.'[34] However, considering that numerous limitations may be imposed on these rights[35] and that their enforcement relies on aware and proactive data subjects, the use of the term 'control rights' should be used with caution in both academic and policy debates. The term 'control rights' assumes and implies that data subjects can exercise control over their personal data, whereas, in practice, this control is conditional, can be limited and may be unfeasible due to the large amount of simultaneous operations processing personal data of individuals being conducted by multiple actors. This being said, it must be acknowledged that data subjects in the EU are becoming increasingly aware about their data subject rights.[36]

The Senegalese data protection law in Article 37 foresees numerous data subject rights. Each of them will be discussed in a separate sub-section.

a) The right to information

According to Article 58 of the Senegalese data protection law, data controllers must inform data subjects of the processing they intend to conduct. In situations where personal data are collected directly from the person concerned, the data controller must provide at the time of collection through whatever means and media used, the following information:

1) the identity of the controller and, where appropriate, his representative;
2) the specific purpose or purposes of the processing for which the data are intended;
3) the categories of data concerned;
4) the recipient(s) or categories of recipients to whom the data are likely to be communicated;
(5) whether the answer to the questions asked is mandatory or optional and possible consequences of a failure to respond;
6) the possibility of requesting to no longer appear on the file;
7) the existence of a right of access data concerning them and rectification of such data;
8) the "shelf life" of the data (retention period);
9) where appropriate, transfers of personal data envisaged to third countries.

Such information notices are not necessary in situations where:

---

[34] European Union Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ EC (GDPR) Recital 7.

[35] Such limitations are of these rights foreseen in the provisions establishing the rights of data subjects. Also, according to Article 23 on retractations, limitations to data subjects' rights may be adopted at national or EU level if they 'respect the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard.'

[36] see, Special Eurobarometer 487a, The General Data Protection Regulation, 2019.

1) the data collected and used in an operation implemented on behalf of the State and involving State security, defence, public security or the object of the execution of criminal convictions or security measures, insofar as such limitation is necessary to respect the ends pursued by the processing operation;[37]
2) where processing is necessary for prevention, research, finding and prosecution of any offense;
3) where the processing is necessary to take into account an economic interest or significant financial contribution by the State, including in the monetary, budgetary, customs and tax.

From the EU perspective, the restriction of the right to information as well as other data subjects' rights may take place only if it 'respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard.'[38]

a. The right to access

According to Article 62 of the Senegalese data protection law, data subjects, who can prove their identity, may ask (in writing) data controllers to give them access to their personal information. More specially, data subjects can ask to receive:
1) information to know and challenge the processing;
2) confirmation that personal data concerning him or her are being processed;
3) the communication, in an accessible form, of personal data which is being processed as well as any available information regarding the origin of such data;
4) information relating to the purposes of the processing, the categories of data processed and the recipients or categories of recipients to whom the data are communicated;
5) where appropriate, information on the transfer of personal data to a third country.

The right to access also allows data subjects to attain a copy of the personal data concerning them. The controller, however, may charge for a copy an amount which may not exceed the cost of reproduction. In case of dispute, the burden of proof lies with the controller to demonstrate that the right of access is exercised.
If there is a risk of concealment or disappearance of the personal data, the concerned data subject may inform the CPD and request it to take any measure likely to prevent such concealment or disappearance. Additionally (as prescribed in Article 64 of the Senegalese data protection law), if the concerned data subject, when exercising the right of access, considers

[37] The requirement 'on behalf of the State' cannot be implicit. There must be either a law governing such processing, or a contractual arrangement set in place between the state and the controller.
[38] Article 23.1, GDPR.

that the data communicated by the controller do not comply with the data processed, then he or she can notify the CPD for further investigation.

Article 65 of the Senegalese data protection law includes an unusual provision,[39] according to which: *The right of access of a patient is exercised by the patient himself or through a doctor he designates. If the patient is dead, the access can be granted to his non-separated spouse, children, and parents.*

b) The right to object

Article 68 of the Senegalese data protection law allows data subjects to object the processing of their personal data if they have a legitimate reason, unless the processing is carried out to meet a legal obligation of the controller.

c) The right to request rectification

According to Article 69 of the Senegalese data protection law, data subjects, who can prove their identity, can ask the controller to rectify, supplement, update, block or delete personal data concerning them which are inaccurate, incomplete, equivocal, out of date, or of which the collection, use, disclosure or storage are prohibited.

Where the interested party so requests in writing, whatever the medium, the controller must justify, at no cost to the applicant, that he has carried out the required operations mentioned above within one month after the registration of the request.

If data has been passed on to a third party, the controller must perform the necessary actions to notify the third party of the transactions carried out in accordance with the data subject's request.

14. International data transfer

Following the EU approach, the Senegalese data protection framework prohibits transferring personal data to third countries. Exceptions to the prohibition are foreseen in situations, where such countries provide for a sufficient level of protection of private life, freedoms and fundamental rights of individuals with respect to the processing of their personal data (Article 49 of the Senegalese data protection law). It should be highlighted that prior to any transfer of personal data to a third country, the controller must notify the CPD, so the authority receives assurances about such transfer from the responsible individual within the entity.

[39] The EU data protection framework concerns only identified or identifiable, living individuals.

Furthermore, the controller can transfer personal data to a third country or third parties that do not fulfil the conditions set out in Article 49 of the Senegalese data protection law if the transfer is *ad hoc*, and if the transfer is necessary under one of the following conditions:

1) to safeguard the life of the data subject;

2) to safeguard the public interest;

3) to fulfil obligations to ensure the recognition, exercise or defence of a right to justice;

(4) to enter into a contract between the controller and the person concerned or meet their contractual obligations.

15.Notification to CDP

The data controller must either notify the CDP or obtain authorisation from the CDP before processing data.[40]

According to Article 20, controllers who seek to process genetic and biometric data, data on health research, data on personal identity number or other general identifiers, historical, statistical, and scientific data; and data of notable public interest need to obtain CPD's authorization to process such personal data. The CPD's website provides access to several templates of notification forms.[41] Controllers must select the template that reflects their processing operations. According to Article 22, in order to obtain authorisation controllers are asked to provide detailed information about the purpose(s) of processing, interconnection and linking of data involved, recipient(s); security measures; and a possibility of a transfer outside the country.

It must be noted that by law (Article 23), CPD may take up to two months to review a request, upon receiving a notification form. This period may be prolonged by a reasoned decision of the Commission. If the request for authorization has not been approved within the period of two months, then the controller can proceed with the processing, assuming that the authorisation request has been accepted.

16.Summary

[40] The notification system was foreseen in Articles 18 and 19 of the Data Protection Directive. It was replaced by accountability measures and an obligation to document processing operations in the GDPR as it was deemed to be outdated and not to assist individuals, when implementing their rights.

[41] Forms are available: https://www.cdp.sn/liste-des-formulaires.

In view of the anticipated deployment of the Nyss platform in Senegal and the consequent transfer of data between Senegal and the cloud services platform based in the EU, the present gap analysis aims to compare the Senegalese and European data protection frameworks, pointing out their similarities and discrepancies.

As the Senegalese data protection law was inspired by the EU Data Protection Directive 95/46/EC (the predecessor of the General Data Protection Regulation (EU) 2016/679), many key concepts and principles are defined in similar terms in both the Senegalese and the European data protection frameworks. In particular, both laws emphasise the transparency principle by requiring controllers to provide data subjects with meaningful and elaborate information concerning the processing of their personal data.

The GDPR, however, contains certain concepts that are not included in the applicable Senegalese data protection framework and further details some principles and rights, in comparison to its Senegalese counterpart. For example, the GDPR requires controllers to notify data breaches to national data protection authorities and, when relevant, to data subjects. The GDPR also requires controllers to implement data protection by design and by default principles and to conduct data protection impact assessments (DPIA) in situations where the processing operations may result in a high-risk to individuals' rights and freedoms, whose personal data is subject to the processing. In comparison to the Senegalese data protection law, the GDPR considerably extends requirements for processors, who alike the controllers, are now required to keep documentation of their processing activities, ensure security of personal data and (in certain situations) to appoint a data protection officer.

For the most part, both frameworks are compatible, however, regarding the few discrepancies that exist (e.g., a notification requirement and rights of data subjects), controllers in Europe and Senegal will have to work together to ensure the most protection for data subjects in processing operations that will involve the transfer of data between countries.

Finally, it should be noted that a proposal to replace the 2008 Senegalese data protection law was published in 2019. The proposal seeks to address governance issues (i.e., the set-up of CPD) as well as to better respond to specific issues (e.g., video surveillance) and key emerging digital issues (e.g., artificial intelligence and cloud computing). Public consultations on the proposal are ongoing and it remains to be seen whether, and to what extent, the revised Senegalese data protection law will include new requirements introduced in the GDPR.

***