Data Protection in Africa | Country Briefs

Tara Davis

July 2021

Table of contents

BURKINA FASO

As at 10 September 2020

COUNTRY OVERVIEW			Ref
Is there a comprehensive data protection law?	☒	The Protection of Personal Data Act 010-2004/AN (2014).	Law link
Does the law establish a supervisory authority?	☒	The Law establishes the *Commission de l'Informatique et des Libertés (CIL)*.	Article 26
Does the law define the term "personal information"?	☒	The term "personal information" is defined in Article 2 of the Law.	Article 2
Does the law prohibit the processing of certain types of personal information?	☒	As a general principle, the Law prohibits the processing of certain types of personal information, referred to as "special personal information". This is subject to certain exceptions.	Article 20
Does the law prescribe its scope of application?	☒	The Law applies to all entities regardless of the identity of the data controller. Foreign entities, which are not domiciled in Burkina Faso but have access to means of processing there, must comply if they do more than simply forward personal information through Burkina Faso.	Articles 4; 8
Does the law apply extra-territorially?	☐	No.	N/A
Does the law set out conditions for the lawful processing of personal information?	☒	The Law outlines at least five conditions for the lawful processing of personal information.	Chapter 1
Does the law stipulate the requirements for valid consent?	☐	The Law does not specify requirements for valid consent.	N/A
Does the law require notification in the event of a data breach?	☒	In the event of a data breach of personal information, the Law only specifies notification of the third party who has accessed the data.	Article 16
Can personal information be transferred to a third party in a foreign country?	☐	Data may only be transferred to a foreign country if it is subject to the same level of protection there.	Article 24
Does the law require a data protection impact assessment to be conducted?	☐	The Law does not provide for impact assessments.	N/A

Does the law require data processing registers?	☒	Yes.	Article 44
Does the law prescribe the use of terms of service icons?	☐	No.	N/A
Does the law prescribe penalties for non-compliance?	☒	The Law provides for criminal penalties for non-compliance.	Title 4

LEGAL ANALYSIS

Legal framework

The Protection of Personal Data Act 010-2004/AN of 2014 ('the Law') was enacted to protect human rights in Burkina Faso by regulating the treatment of personal data.

It was signed into law on 20 April 2004 and Burkina Faso became the first French-speaking country in Sub-Saharan Africa to have an operational data protection authority in 2007. Promulgation of the law required all entities to be compliant within three years for data processing by state entities and 6 months for all other entities.

The Law states that the sanction powers of the Supervisory Authority, the Commission for Informatics and Freedoms, are specified by regulations, as are regulations that mandate the handling of data processing by state agencies. The Law makes mention of these regulations in Articles 18 26 but we have been unable to find any publicly available regulations.

Key definitions

The definitions are set out in Chapter 1 of the Law. In terms of the relevant role players, the key definitions include the following:

- The term ***"data controller"*** means the natural or juristic person, public or private, who has the power to make decisions about the creation of personal data.

- The term ***"recipient"*** of the processing of personal data means any natural or juristic person, public or private, other than the data subject, empowered to receive communication of data.

- The term ***"data subject"*** means the identifiable person to which the personal data refers.

The following definitions are also of relevance:

- The term ***"personal data"*** is defined to mean:
  "any information that permits, in any form, directly or indirectly, the identification of natural persons, notably by reference to an identification number or to multiple elements specific to their physical, psychological, philosophical, economic, cultural or social identities".

- The term "***processing of personal data***" is defined to mean:
  "Any operation or collection of operations effected with or without the aid of automatic processing by a natural or juristic person and applied to personal data, such as the collection, recording, extraction, consultation, utilisation, disclosure by transmission, sharing or any other form of provision, merging or interconnecting, blocking, erasure or destruction".

Scope of application

Requirements for the scope of application

The Law applies to "any processing, automated or otherwise, of personal data contained in or intended to form part of a filing system for which the data controller is established in the territory of Burkina Faso, or, if not established there, has recourse to methods of processing situated in the territory of Burkina Faso, with the exclusion of data that is not utilised except for transit purposes." This raises the following considerations:

- ***Processing of personal information:*** there must be processing of personal data.

- ***Entry into a record:*** the personal data must be a part of or intended to be a part of a filing system.

- ***Automated or non-automated means:*** it is irrelevant whether the data controller makes use of automated or non-automated means.

- ***Domicile in Burkina Faso:*** it is irrelevant whether the data controller is domiciled in Burkina Faso, provided that the data controller has recourse to means of processing in Burkina Faso. The Law does not apply if those means are only used for transit purposes through Burkina Faso.

What information does the law apply to?

The Law applies to "any information that permits, in any form, directly or indirectly, the identification of natural persons, notably by reference to an identification number or to multiple elements specific to their physical, psychological, philosophical, economic, cultural or social identities".

Compliance by responsible parties

The processing of personal information must be declared to the CIL prior to processing, except for some exclusions provided for in the Law, such as processing carried out for exclusively personal or domestic purposes.

The CIL establishes and publishes simplified standards for the most common categories of data processing of a public or private nature which do not materially interfere with privacy or personal freedoms. For such types of processing, a data controller need only to file a simplified declaration of compliance with one of these standards with the Commission.

Authorisations for the processing of personal data by state entities is decided by decree of the CIL.

Compliance by operators

The Law does not mention its application to operators.

Exclusions

The Law provides for certain exclusions from its scope of application. The exclusions include the following:

- ***Temporary copies***: the provisions of the Law do not apply to temporary copies that are made within the scope of transmission and provision of access to a digital for the sole purpose of enabling other recipients of service the best possible access to information.

- ***Research in the field of health*****:** the processing of individual-related data for research purposes in the domain of health are subject to the provisions of the Law but are not subject to the provisions on consent, notification of the purpose of processing, regulations on the automatic processing of data by public bodies, and consent for sensitive data (Articles 5, 13, 18 and 20). Requests for processing health data must be submitted to the CIL and is subject to the favourable opinion of the Ethics Committee for Health Research. There are additional exclusions for the use of data for health research in Article 56.

- ***Health data:*** processing of data for the purpose of therapeutic or medical monitoring of individual patients is not subject to the Law. The same applies to processing that enables research to be carried out with that data provided the research is carried out by the persons providing the monitoring and is intended for their exclusive use. Any disclosure or commercial exploitation of personal health data is prohibited.

- ***Use of data by the media:*** Articles 20, 22 and 24 (regarding special personal data, judicial and criminal information and transborder data transfers) do not apply to the processing of personal data by the written or audio-visual press within the framework of the laws that govern them if their application would have the effect of limiting the exercise of freedom of expression.

- ***State security information:*** The government may issue decrees stating that regulations about the processing of certain data concerning state security, defence and public security will not be published.

Rights of data subjects

The Law sets out the rights of data subjects, which includes the following:

- ***Consent:*** any processing of personal data must receive the consent of the data subject(s), except for the exemptions provided by the Law.

- ***Access:*** data subjects are entitled to know about information and reasoning used in processing, automated or otherwise. They also have the right to know about any preserved data that concerns them, and they must be able to exercise this right without delay or excessive fees. Information regarding health data must be communicated to them by an intermediary doctor appointed for this purpose.

- ***Challenge***: data subjects have the right to challenge the information or reasoning used in processing, automated, or otherwise, the results of which they oppose. They also have the right to oppose the processing of data relating to them for legitimate reasons.

- ***Automated decision-making:*** data subjects have the right not to be subject to automatic decision-making. This right extends to decisions made by any court, administration or decisions made privately.

- ***Notification:*** data subjects have the right to be notified about the purpose of the processing, the recipients of the data, the obligatory or optional nature of the answers to the questions asked as well as the possible consequences of a default response. This provision does not apply to the collection of data for the establishment of an infringement or offence.

- ***Correction:*** if data is incomplete or incorrect, data subjects have the right to ask for a correction or adjustment, in which case the data controller must make the correction or adjustment and deliver a copy of the modified recording without fees. A different process applies to processing involving state security, defence, and public security.

Conditions for the lawful processing of personal information

Chapter 1 Title II outlines the general conditions for the lawful processing of personal data. Responsible parties are obligated to collect and process personal data in a manner that is fair, lawful and not fraudulent.

The Law prescribes that lawful processing of personal data can only occur under the following conditions:

- ***Purpose Specification:*** the data must be collected for specific, explicit and legitimate purposes and cannot be used for any other purposes.

- ***Notification:*** responsible parties are obligated to notify data subjects about the purpose of the processing, the recipients of the data, the obligatory or optional nature of the answers to the questions asked as well as the possible consequences of a default response. This last provision does not apply to the collection of data for the establishment of an infringement or offence.

- ***Processing limitation:*** the data must be appropriate, relevant and not excessive with regard to the purpose for which they were collected and later processed.

- ***Time Constraints on Storage:*** the data must only be retained for a duration that does not exceed the period necessary for the purpose for which it was collected and processed. Beyond this, the data may only be kept in a non-identifiable form with a view to processing for historical, statistical or research purposes.

- ***Security Safeguards:*** The data controller must enforce all appropriate technical and organisational measures to preserve the security of the data, notably protecting their accidental or illicit destruction, accidental loss, alteration, distribution or unauthorised access.

Restrictions on the processing of personal information

Special personal information

The Law prohibits the collection or processing of special personal data without the express consent of the data subject. Special personal data includes personal information relating to a person's health or which reveals racial or ethnic origins, political, philosophical or religious opinions, union membership or customs/morals.

Automated decision-making

The Law provides that a data subject may not be subject to any court, administrative or private decision involving an assessment of human behaviour that has as its sole basis the automated processing of information that gives a characterisation of the profile or the personality of an interested party intended to assess certain aspects of their personality.

Automated processing of personal data on behalf of the state, a public entity, a local authority or a juristic person governed by private law and managing a public service are decided by decree after reasoned approval of the CIL. In the case of an unfavourable opinion from the CIL, an appeal may be brought before the Council of State.

Data relating to offences, convictions and security measures

Only the following entities may process personal data relating to offences, convictions and security measures:

- The courts and public authorities acting within the framework of their legal powers;
- Legal persons managing a public service, after approval from the CIL;
- Court officers, as required for the exercise of their duties.

Transborder data transfers

The Law prohibits the transfer of personal data in any form outside of the Burkinabé territory for the purpose of automatic processing, subject to certain exceptions.

The prohibition on transborder data transfers does not apply if one or more of the following exceptions is applicable:

- ***Adequate level of protection:*** the processing is done under the same protections as are afforded by Burkina Faso's law;

- ***Approval from the CIL:*** in exceptional circumstances, processing may be authorised by decree after approval from the CIL.

Requirements for consent

Other than the exemptions below, the Law requires that any processing of personal data must receive the consent of the data subject(s).

Personal data processing can be done without the consent of the data subject in the following cases:

- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary for safeguarding the life of the data subject or a third party;
- The processing relates to data made public by the data subject;
- The processing is necessary for the execution of a contract to which the data subject is a party, or to precontractual measures taken at the latter's request;

- The processing is necessary for the establishment of an infringement, right, exercise or the defence of a legal right;
- The processing is necessary for the purposes of preventative medicine, diagnostic medicine, administration of care or treatment, or management of health services, provided that they are implemented by a member of the health profession or by another person who is bound by professional confidentiality.

Transparency

Openness

Articles 5 and 12 requires that everyone must be informed that their data will be processed for a given purpose, and that this processing can only take place with their consent. An exception is provided for data collected for the purpose of establishing an infringement.

With regards to data that concerns national security, defence or public security, requests to access information must be addressed to the CIL who will designate one of its members from the judiciary to conduct investigations and make the necessary modifications. The applicant must be notified that the modifications have been carried out.

Notification of a data breach

Article 16 pertains to openness in the case of accidental sharing of information with a third party. In such a case, the data controller is required to send the third party a notice of rectification and cancellation, unless this requirement has been dispensed with by the CIL. Data subjects have the right to oppose the processing of data relating to them for legitimate reasons.

There is no obligation to notify a data subject in the event of a breach.

Impact assessments

The Law does not require impact assessments.

Data processing registers

The CIL publishes a list of data processing types that specifies for each:

- the law or regulatory act mandating its creation or the date of its declaration, its name and its purpose,
- the service to which the right of access is exercised,
- the categories of identifiable information recorded as well as the recipients or categories of recipients authorized to receive communication of this information.

Terms of service icons

The Law does not require the use of terms of service icons.

Additional transparency obligations

In addition to the above, the CIL is required to present an annual report to the President of the country, the President of the National Assembly and the President of the Constitutional Council, which is also made public and serves to enhance transparency.

Participation

Data subject participation

The Law provides in various sections for the right of the data subject to participate. The Law provides for the following:

- ***Access to personal information:*** A data subject has the right know about information and reasoning used in processing, automated or otherwise, the result of which they are opposed to. They also have the right to know about any retained data that concerns them and they must be able to exercise this right without delay or excessive fees. Information regarding health data must be communicated to them by an intermediary doctor appointed for this purpose.

- ***Challenge***: the right to challenge the information or reasoning used in processing, automated, or otherwise, the results of which they are opposed to. They also have the right to oppose the processing of data relating to them for legitimate reasons.

- ***Notification:*** the data subject has the right to be notified about the purpose of the processing, the recipients of the data, the obligatory or optional nature of the answers to the questions asked as well as the possible consequences of a default response. This provision does not apply to the collection of data for the establishment of an infringement/offence.

- ***Correction:*** if data is incomplete or incorrect, data subjects have the right to ask for a correction or adjustment, in which case the data controller must make the correction or adjustment and deliver a copy of the modified recording without fees. A different process applies to processing involving state security, defence, and public security.

Policy participation

The CIL is required to stay abreast of updates in the sector and the effects of the use of technology on the right to privacy, the exercise of freedoms and the functioning of democratic institutions.

The CIL is also empowered to propose legislative or regulatory measures to government that aim to protect freedoms in response to technological developments.

Enforcement

Supervisory authority

The Law establishes the *Commission de l'Informatique et des Libertés* (the Commission for Informatics and Freedoms). The CIL is an independent entity responsible for ensuring compliance with the provisions of the law, in particular by informing all those concerned of their rights and obligations and by monitoring the application of the law. To this end, the Commission has regulatory power and a power of sanction which is specified by decree. The Law states that the CIL "may take all necessary measures" to ensure that all processing of identifiable information is implemented in compliance with the Law.

In the exercise of their powers, the members of the CIL do not receive instructions from any authority. The CIL's mandate includes the following:

- To take individual or regulatory decisions if necessary;
- Charge its agents to carry out on-site verifications or demand any information or documents necessary for its mission;
- To issue model rules to ensure the security of systems, and in exceptional circumstances prescribe security measures, particularly regarding the destruction of information or the suspension of authorisations;
- Send warnings and denouncements of offences of which it is aware and ensure that the rights to access and rectification as included in the Law do not hinder the implementation of the Law;
- Establish and publish simplified standards for the most common categories of data processing of a public or private nature which do not involve interference with privacy or liberties.

The CIL presents an annual report to the President of the country, the President of the National Assembly and the President of the Constitutional Council, which is also made public.

Criminal offences

A wide range of criminal offences are created under the Law, which apply to non-automatic use of data except where explicitly mentioned. Some of these include failure to comply with the notification requirements around automatic processing of personal data, unauthorised disclosure of data, failing to take adequate precautions to protect the security of data, and accessing personal data without authorisation. These crimes are punishable by fines and imprisonment up to 5 years.

Obstructing the work of the Commission, by for example refusing on-the-spot verifications, refusing to provide or concealing information and documents, or misleading the Commission is punishable by a fine and up to one year imprisonment.

Civil remedies

Civil remedies are not provided for in the Law.

Administrative fines

The Law does not provide for administrative fines.

Offence	Category	Consequence
Failure to comply with the notification requirements around automatic processing of personal data	Criminal	Imprisonment of between three months and five years and a fine of between 500,000 and 2,000,000 francs CFA
Automatic processing of data without taking the necessary security precautions such as allowing them to be communicated to a third party without authorisation	Criminal	Imprisonment of between three months and five years and a fine of between 500,000 and 2,000,000 francs CFA
Unauthorised sharing of data with a third party or accessing data without authorisation	Criminal	Imprisonment of between three months and five years and a fine of between 1,000,000 and 3,000,000 francs CFA
Misuse of the data relative to its stated purpose	Criminal	Imprisonment of between three months and five years and a fine of between 500,000 and 2,000,000 francs CFA
Collecting data in a fraudulent, unfair or illegal manner or processing data about a natural person against their will if they have legitimate complaints	Criminal	Imprisonment of between three months and five years and a fine of between 2,000,000 and 5,000,000 francs CFA

Automatic processing of data for the purpose of health research without informing data subjects of their rights to access, correct and challenge the nature of the information of the recipients	Criminal	Imprisonment of between three months and five years and a fine of between 2,000,000 and 5,000,000 francs CFA
Automatic processing of data for the purpose of health research against the will of the data subject or without clear and express consent, or, in the case of a deceased person, against their wishes expressed in their lifetime.	Criminal	Imprisonment of between three months and five years and a fine of between 2,000,000 and 5,000,000 francs CFA
Placing or keeping special personal data in digital storage without express consent of the data subject (outside the provisions of the law)	Criminal	Imprisonment of between three months and five years and a fine of between 500,000 and 2,000,000 francs CFA
Placing or keeping identifiable data concerning offences, convictions, or security measures in digital storage (outside the provisions of the law)	Criminal	Imprisonment of between three months and five years and a fine of between 500,000 and 2,000,000 francs CFA
Keeping identifiable data without the permission of the CIL beyond the period stated at the time of the declaration	Criminal	Imprisonment of between three months and five years and a fine of between 500,000 and 2,000,000 francs CFA
Disclosing identifiable information, the disclosure of which would undermine the honour or privacy of a data subject, without authorisation of the interested party to a third party who is not authorised to receive the data. Prosecution can only be brought on complaint of the victim, their legal representative or their dependents	Criminal	Imprisonment of between three months and five years and a fine of between 1,000,000 and 3,000,000 francs CFA
The same offence as the above committee through recklessness or negligence. Prosecution can only be brought on complaint of the victim, their legal representative or their dependents	Criminal	Imprisonment of between three months and five years and a fine of between 500,000 and 2,000,000 francs CFA

Obstruction of the CIL's actions by opposing on-the-spot verifications, refusing to provide information or documents or providing misleading, incorrect or unintelligible information	Criminal	Imprisonment of between one month and one year and a fine of between 200,000 and 1,000,000 francs CFA

CABO VERDE

As at 5 October 2020

COUNTRY OVERVIEW			Ref
Is there a comprehensive data protection law?	☒	The Data Protection Act, Law 133 of 2001	DPA link
Does the law establish a supervisory authority?	☒	Yes, the National Data Protection Commission (CNDP).	Article 22
Does the law define the term "personal information"?	☒	The term "personal data" is defined but it does not include a list of the types of information included. It applies to an identifiable data subject which may be identified by an identification number or by means of one or more specific elements of their physical, physiological, psychological, economic, cultural or social characteristics.	Article 5
Does the law prohibit the processing of certain types of personal information?	☒	As a general principle, the DPA prohibits the processing of certain types of personal information, referred to as "sensitive data", subject to certain exceptions such as the provision of consent or that it has been authorised by law.	Article 8
Does the law prescribe its scope of application?	☒	The DPA applies to persons, public authorities, services or any other entity which processes personal data. It applies to controllers outside of Cabo Verde if Cabo Verdean law applies or equipment in Cabo Verde is used for more than just transit purpose.	Article 2
Does the law apply extra-territorially?	☐	The law is unclear; Article 4 of Law 42 notes that the CNPD exercises its authority in Cabo Verde but may act outside of that scope when requested to do so by a supervisory authority in a foreign state or in the defence or exercise of rights of individuals who live abroad.	Article 4 of Law 42
Does the law set out conditions for the lawful processing of personal information?	☒	Yes, the DPA sets out seven conditions and obligations for lawful processing.	Chapter II

Does the law stipulate the requirements for valid consent?	☒	Yes, it must be a free, specific and informed expression of will.	Article 5(1), as amended by Law 41.
Does the law require opt-in consent?	☐	No.	N/A
Does the law require notification in the event of a data breach?	☐	No.	N/A
Can personal information be transferred to a third party in a foreign country?	☐	As a general principle, the DPA prohibits the transfer of personal data to a third party in a foreign country. This is subject to certain exceptions.	Article 19; Article 20
Does the law require a data protection impact assessment to be conducted?	☐	No.	N/A
Does the law require data processing registers?	☒	Yes.	Article 27
Does the law prescribe the use of terms of service icons or an equivalent measure to inform consent of data use?	☐	No.	N/A
Does the law prescribe penalties for non-compliance?	☒	The DPA provides for criminal, civil and administrative penalties for non-compliance.	Chapter VI

LEGAL ANALYSIS

Legal framework[1]

The Data Protection Act No. 133/V/2001 of 22 January 2001 (the DPA) was enacted to establish a framework for the protection of individuals concerning the processing of personal data.

The Law came into force 30 days after publication on 22 January 2001. Controllers who processed data held in manual filing systems were given 6 months to comply with the provisions concerning sensitive personal data, the conditions for lawful processing and data subject rights. Controllers of automated files had one year to comply.[2]

The legal framework further comprises Law 41/VIII/2013 of 17 September 2013 (Law 41) which amends the DPA and is only available in Portuguese. Law 42 /VIII/2013 of 17 September 2013 (Law 42) is also applicable and regulates the governance of the data protection authority, the National Commission of Data Protection (CNDP).

Key definitions

The definitions are set out in Article 5 of the DPA. In terms of the relevant role players, the key definitions include the following:

- The term ***"controller"*** is defined to mean the person or group, public authority, service or any other entity which alone or jointly with others determines the purposes or the means for the processing of personal data.

- The term ***"sub-contractor"*** is defined to mean a natural or legal person, a public authority, agency or any other entity that processes personal data on behalf of the controller.

- The term ***"third party"*** is defined to mean a person or group, a public authority, agency or any other entity other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data.

- The term ***"recipient"*** is defined to mean a person or group, a public authority, agency or any other entity to whom personal data are disclosed, whether a third party or not;

---

[1] Law 133 is drafted in Portuguese and although we used an official English translation, we have picked up on discrepancies between the English and Portuguese versions. Law 42 was only available in Portuguese and we accordingly used an internal translation.

[2] Note: the Portuguese version of the law provides for a period of 1 year; the English version provides for 6 months.

however, authorities which may receive data in the framework of the law shall not be regarded as recipients.

The following definitions are also of relevance:

- The term ***"personal data"*** is defined to mean any information of any type or nature and irrespective of the medium involved, including sound and image relating to an identified or identifiable person, the "data subject". Article 5(2) notes that a person is considered identifiable if they may be directly or indirectly identified by an identification number or by means of one or more elements of his physical, physiological, psychological, economic, cultural or social characteristics.

- The term "***processing of personal data"*** or ***"processing"*** is defined to mean any operation or set of operations which is performed upon personal data, whether wholly or partly, with or without automated means, such as: collection, recording, organisation, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment, or combination, as well as blocking, erasure or destruction.

Scope of application

Requirements for the scope of application

Article 2 of the DPA sets out the scope of application, which states that it applies to the processing of personal data wholly or partly by automated means as well as to the processing of personal data other than by automated means contained in manual files.

This raises the following considerations:

- ***Processing of personal information:*** there must be processing of personal data.

- ***Contained in manual files:*** the personal data must be contained in or form part of manual files.

- ***Automated or non-automated means:*** it is irrelevant whether the controller makes use of automated or non-automated means.

Article 2 further states that the DPA applies in the following instances:

- processing is carried out by a controller situated in Cape Verde;

- processing is carried out outside Cape Verde but in places where Cape Verdean law applies by virtue of international public law;
- processing is carried out by a controller outside of Cape Verde but who makes use of equipment situated in Cape Verde for anything other than transit purposes. In this instance, the controller is required to designate someone within Cape Verde to replace him in all his rights and obligations, by notice to the CNDP. This does not absolve the controller of liability.

Article 2(4) notes the DPA's application to video surveillance and other forms of sound and images which identify people. The DPA will apply to this data if the controller is based in Cape Verde or uses a computer or data communication network access provided in Cape Verde.

What information does the law apply to?

The DPA applies to any information of any type and nature irrespective of the medium involved, relating to an identified or identifiable person, the "data subject". A person is considered identifiable if they may be directly or indirectly identified by means of an identification number or by means of one or more specific elements of their physical, physiological, psychological, economic, cultural or social characteristics.

The DPA also applies to video surveillance and other forms of capture – including images and sound which may identify people.

It also applies to data relating to public security, national defence and State security, subject to legislation and international law to which Cape Verde is bound.[3]

Compliance by controllers

Article 6(3) notes that the data controller is responsible for ensuring compliance with the conditions for lawful processing. The DPA does not explicitly state which types of entities fall within its scope but is broadly defined to include persons, public authorities and all other entities.

The Law applies to all controllers processing within Cabo Verde or in a territory bound by Cabo Verdean law, or any controller, outside of Cabo Verde, who makes use of equipment situated in the territory for anything other than transit purposes.

Controllers are bound by professional secrecy, even after their functions or mandates have ended.

[3] Note: this is contained in article 2(4) of the official English translation but the word 'apply' has been omitted. It notes "This Act/Law shall to the processing of personal data regarding public safety […]" It is possible that it should read that the law does not apply to these sectors, but it is unlikely.

Compliance by subcontractors

A subcontractor is defined in Law 41 but the role is referred to as a processor in the DPA.

When processing is carried out on behalf of a controller, the controller must choose a subcontractor that provides sufficient guarantees in terms of technical security and organisational measures and must ensure compliance with them. The processing must be governed by a contract that stipulates that the subcontractor only acts on instruction from the controller and that they are bound by the same obligations.

Exclusions

The Law provides for only one exclusion from its scope of application, which is when data is processed in the course of personal and household activities.

Rights of data subjects

Section II, Article 11 of the DPA prescribes the rights of data subjects, which include the following:

- ***Information:*** the data subject has the right to be notified that their data is being collected. The DPA specifies what information must be communicated to the data subject, some of which includes the controller's identity, the purpose for processing it and the nature of replies. The right notes that where data is collected from open networks, the data subject must be informed that their information may be circulated without security measures and is accordingly at risk of being used by unauthorised parties. This right may be waived for state security, crime prevention or investigation purposes and does not apply for artistic or literary expression.

- ***Access:*** the data subject has the right to confirm whether their data is being processed; access information concerning data and its source; and to access information concerning the logic involved in automatic processing. Article 12(1) notes that the data subject is entitled to this without constraint, excessive delay or expense.

- ***Automated decision-making:*** the data subject has the right to know the logic involved in any automated processing of data relating to them, and not to be subject to a decision based solely on automated processing that produces legal effects or significantly affects them. It specifically includes evaluations concerning a data subject's work performance, creditworthiness, reliability or conduct. Decisions taken in the course of a contract are excluded, and those authorised by the CNPD.

- ***Correction, erasure or blocking:*** the data subject has the right to request the correction, erasure, or blocking of the processing of their personal data if it is incomplete, inaccurate or does not comply with the law.

- ***Objection:*** the data subject has the right to object to the processing of their personal data on compelling, legitimate grounds, and to be offered the opportunity to expressly object to the processing of their data for direct marketing or any other research, free of charge.

Conditions for the lawful processing of personal information

The DPA states that the processing of personal data shall be carried out transparently and with strict respect for privacy and other fundamental rights, freedoms and guarantees of the citizen.

Beyond that, Chapter II sets out the conditions for the lawful processing of personal data, which include:

- ***Legality:*** data must be processed lawfully and with respect for the principle of good faith;

- ***Purpose specification:*** data must be collected for specific, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes;

- ***Processing limitation:*** data must be adequate, relevant and not excessive in relation to its purpose;

- ***Data quality:*** data must be accurate, kept up to date and adequate measures must be implemented to ensure that incorrect or incomplete data is erased or rectified;

- ***Retention period limitation***: data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which they were collected or for which they are further processed. Data may be further processed for historical, statistical or scientific purposes or may be stored longer if authorised by the CNPD in instances of legitimate interest, so long as it does not compromise the rights and freedoms of the data subject;

- ***Security safeguards:*** Article 15 requires that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, or any other unlawful processing.

- ***Data subject participation:*** Article 7 notes that personal data may only be processed if the data subject has unambiguously consented unless one of the following applies:

- ***Contract:*** processing is necessary for the performance of a contract to which the data subject is party;
- ***Legal obligation***: processing is necessary for compliance with a legal obligation to which the controller is subject;
- ***Vital interests:*** processing is necessary for the protection of the vital interests of the data subject who is physically or legally incapable of providing consent;
- ***Public interest:*** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority;
- ***Legitimate interest***: processing is necessary in pursuit of the legitimate interests of the controller or third party, except where such interests are overridden by the interests, rights and freedoms of the data subject.

Combining personal data from different controllers or that was collected for different purposes must receive prior authorisation from the Parliamentary Committee of Investigation.

Restrictions on the processing of personal information

Sensitive data

The processing of personal data revealing philosophical, ideological or political beliefs or punishments, religion, political party or trade union affiliation, racial or ethnic origin, privacy, health or sex life, including genetic data, is prohibited, except in the following circumstances:

- ***Consent:*** if the data subject has given express consent with the guarantee of non-discrimination;

- ***Legal authorisation***: authorisation provided for by law is foreseen with the guarantee of non-discrimination and adequate measures of assurance. Article 8(2) notes that in determining legal authorisation, the indispensability of processing personal data for public interest purposes must be considered.

- ***Statistics:*** the data is processed purely for statistical purposes, and data subjects are not individually identifiable, and provided there are adequate security measures;

- ***Vital interests:*** the processing is necessary to protect the vital interests of the data subject or oanother person if the data subject is physically or legally incapable of giving their consent;

- ***Specific organisation***: the processing is carried out by a foundation, association or non-profit-seeking body with a political, philosophical, religious or trade union aim, and the data subject has consented. The processing must relate solely to the members of the body or to persons who have regular contact with it and the data must not be disclosed to a third party without the consent of the data subjects;

- ***Public:*** processing concerns data which is manifestly made public by the data subject, provided their consent for their processing can be clearly inferred;

- ***Legal claims:*** the processing is necessary for the establishment, exercise or defence of legal claims and is exclusively carried out for that purpose;

- ***Public security:*** processing may take place "when the indispensable security of the state, of public security, and the prevention, investigation or repression of penal infringements are demonstrated." Article 8(5) notes the need for adequate information security measures in this instance.

The processing of personal data relating to health and sex life, including genetic data, is permitted if it is necessary for preventive medicine, medical diagnosis, the provision of medical care or treatment or the management of health-care services. Such processing must be done by a health professional or other person bound by professional secrecy, the CNPD must be notified, and adequate security measures are implemented.

Data concerning the administration of the law

Article 9 concerns the processing of personal data concerning suspicion of illegal activities, penalties, security measures, infringements and criminal and administrative offences. It notes that central registers which process information concerning any of this information may only be created and kept by public entities who are mandated for such activities, and with the authorisation of the CNPD. The article notes that the rights and freedoms of the data subject may not be overridden. In the case of police investigations, only necessary personal data may be processed to prevent a specific danger or to prosecute a particular offence.

Article 16 sets out the special security precautions that controllers of sensitive personal data must take. The CNPD may waive some of these requirements in certain circumstances.

Notifications and requests for authorisation must include detailed information about the controller, the purpose, the types of data used, the length of time the data will be kept, and the security measures to be taken, as detailed in Articles 25 and 26.

Children

The Law makes no special provision for the processing of data relating to children.

Direct marketing

The data subject has the right to object, free of charge, to the processing of personal data relating to them which will be processed for direct marketing or any other form of research, or to be informed before personal data are disclosed for the first time to third parties for the purpose of direct marketing. They also have the right to be expressly offered the right to object, free of charge, to such disclosures or uses.

Automated decision-making

Article 23 obliges the controller or their representative to notify the CNPD before carrying out any wholly or partially automatic data processing operation or set of operations. The CNPD may authorise the simplification of or exemption from notification for particular categories of processing which are unlikely to jeopardise the rights and freedoms of data subjects. An exemption from notification is allowed if the sole purpose of the processing is for the maintenance of a register that is intended to provide information to the public and which is open to consultation by the public in general or by any person demonstrating a legitimate interest.

Transborder data transfers

Personal data may only be transferred to another country if it has an adequate level of data protection. The CNPD determines whether a country has an adequate level of protection, which is assessed in light of all the circumstances surrounding the data transfer. The DPA notes the factors which must be considered, some of which include: the nature of the data, the purpose of the processing and the applicable laws and professional rules of the recipient country.

Transfer of personal data to a state which does not provide an adequate level of protection may still be allowed in the following circumstances if authorised by the CNPD:

- ***Consent:*** the data subject provides unequivocal consent.

- ***Contract performance:*** the transfer is necessary for the performance of a contract between the data subject and the controller or pre-contractual measures requested by the data subject;

- ***Execution of a contract:*** the transfer is necessary for the execution or signing of a concluded or to-be-concluded contract in the interest of the data subject between the controller and a third party;

- ***Public interest:*** the transfer is necessary or legally required on the grounds of important public interest, or for the establishment, exercise or defence of legal claims;

- ***Vital interests:*** the transfer is necessary for the protection of vital interests of the data subject;

- ***Public register:*** the transfer concerns data from a public register which is intended for the information of the public and is open to consultation either by the public or by any person who can demonstrate a legitimate interest.

Article 20(3) notes that the transfer of personal data which is necessary for the protection of State security, defence, public safety and the prevention, investigation and repression of punishable criminal offences is governed by special legal provisions or international conventions to which Cape Verde is party. The DPA does not specify which provisions or conventions apply.

Requirements for consent

The Law defines consent in Law 41 to mean any free, specific and informed expression of will by which the data subject has his personal data processed.

Transparency

The DPA states that the processing of personal data shall be carried out transparently.

Openness

The CNPD must indicate in its annual report all the opinions and authorisations drawn up and granted each year.

Notification of a data breach

The DPA does not require notification of a data breach.

Impact assessments

The DPA does not require the completion of a data protection impact assessment.

Data processing registers

If the processing of personal data is not covered by a legal provision and must be authorised or notified, it must be set down in a CNPD register which is open to consultation by any person. The

DPA specifies that the following information must be included in the register: information concerning the controller; the category of data which is processed; the purpose for processing; the entities to whom it will be disclosed and details concerning the proposed transfer to third countries.

Article 26 notes what information must be specified in the data processing filing system,[4] which incudes:

- Information concerning the controller;
- The category of data which is processed;
- The purpose of processing;
- The entities to whom it will be disclosed;
- The manner of exercising the right of access and rectification;
- Combination of personal data processing;
- Any proposed transfer to third parties.

Terms of service icons

The law does not prescribe the use of terms of service icons, or anything similar.

Additional transparency obligations

- ***Annual report***: Article 27 requires that the CNPD include all opinions and authorisations which were drawn up and authorised to be included in its annual report. The law does not specify that the annual report must be made available to the public.

- ***Publication of judgment***: following an offence, the DPA provides for the publication of the judgment or a public warning of the controller. It requires that publication occurs in a periodical with the largest circulation in the area the infringement occurred and must include a summary of the offense, the penalty, and the identity of the agent. It notes that the cost of publication of the judgment must be borne by the person involved in the judgment and a notice must be affixed for no less than 30 days.

- ***Monthly reports***: Article 45 of Law 42 requires the CNPD to provide monthly reports to the National Assembly concerning its deliberations and activity. An annual report must be sent to the Parliamentary Commission for Fundamental Rights explaining legislative, financial and administrative issues to be discussed. The debate must be released sixty days after receipt of the report.

[4] Note: this filing system is not referred to anywhere else in the DPA; it is submitted that it likely refers to the CNPD register.

Participation

Data subject participation

- ***Access:*** the data subject has the right to confirm whether data is being processed; access information concerning data and its source; and to access information concerning the logic involved in automatic processing. Article 12(1) notes that the data subject is entitled to this without constraint, excessive delay or expense.

- ***Correction, erasure or blocking:*** the data subject has the right to request the correction, erasure, or blocking of the processing of their personal data if it is incomplete, inaccurate or does not comply with the law.

- ***Objection:*** the data subject has the right to object to the processing of their data on compelling, legitimate grounds, and to be offered the opportunity to expressly object to the processing of their data for direct marketing or any other research, free of charge.

- ***Data subject participation:*** Article 7 notes that personal data may only be processed if the data subject has unambiguously consented, subject to exceptions.

Policy participation

Article 12 of Law 42 notes that the CNPD must be consulted on legislative initiatives concerning personal data processing.

Enforcement

Supervisory authority

The DPA establishes the National Data Protection Commission (CNDP). It is an independent administrative authority which operates within the National Assembly. Article 8 of Law 42 notes its power to supervise and monitor compliance with data protection laws and requires that it do so with respect for human rights.

Authorisation from the CNPD is required for the processing of the following information:

- The processing of personal data revealing philosophical, ideological or political beliefs or punishments, religion, political party or trade union affiliation, racial or ethnic origin, privacy, health or sex life, including genetic data in certain circumstances[5];

[5] Note, Article 24 states its application to section 1 (a) and (e) of Article 8, however; Article 8 does not contain 1(e), the ambit of this section is therefore unclear.

- Processing data related to persons suspected of illegal activities, criminal and administrative offences and decisions applying penalties, security measures, fines and additional penalties.
- The processing of personal data for police investigations.

Article 25 specifies what information must be included for applications for opinions, authorisations and notification to the CNPD.

Law 42 regulates the composition, powers, structure and functioning of the CNDP. Article 4 of Law 42 notes that the CNPD exercises its authority in Cabo Verde but may act outside of that scope when requested to do so by a supervisory authority in a foreign state or in the defence or exercise of rights of individuals who live abroad.

Article 6 of Law 41 places a duty of cooperation on all public and private entities which requires they produce all information requested by the CNPD. Members of the CNPD are provided a right to access computer systems and documents concerning the processing of personal data, and the duty to cooperate extends to these items too.

Article 8 of Law 42 provides the CNPD with the following powers:

- ***Investigative powers:*** this power allows the CNPD to access data which is being processed, and collect all information necessary for the performance of its duties;
- ***Powers of authority:*** this power includes the capacity of the CNPD to order the blocking, erasure or destruction of data or to impose a ban on processing;
- ***Opinion:*** this includes the CNPD's power to provide opinions before processing begins and to ensure the opinions are published;
- ***Power to warn:*** this empowers the CNPD to warn or publicly censor processors who have repeatedly failed to comply with provisions. It may also notify the National Assembly, organs of government or authorities.

Article 41 of Law 42 further provides that all representatives of the CNPD can access premises, equipment and services of entities under the supervision of the CNPD. They may further request documents and information for analysis, identify individuals who infringe legislation and collaborate with competent authorities. This may be done within the scope of their duties and they must be able to show proof of such.

The responsibilities of the CNPD are outlined in Article 10 of Law 42, some of which include:

- Authorizing the processing of certain types of data;
- Authorizing the transfer of data to a foreign country;
- Checking the lawfulness of processing at the request of any person whenever such processing is subject to restricted access or information;
- Assessing the claims, complaints or applications of private individuals;
- Applying fines.

Article 10(3) notes that when exercising its function, the CNPD must lay down obligatory decisions which may be challenged or appealed in court. Failure to comply with an individualised deliberation of the CNPD carries a daily fine of CVE 5 000 for individuals and CVE 10 000 for groups.

The CNPD assists in the development of codes of conduct, which take into account the characteristics of different sectors to provide guidelines for the proper implementation of the provisions of the Law. Trade associations and other entities that represent categories of controllers draft the codes and submit them to the CNPD for review, which declares whether they are in accordance with or not.

Members or staff of the CNPD are bound by professional secrecy, even after their functions or mandates have ended.

Enforcement in general

Article 30 specifically notes without prejudice to the right to submit a complaint to the CNPD, any individual may seek recourse regarding the violations of his rights under the DPA.

Article 38 provides that where an offence results from the omission of a duty, the application of a penalty does not release the perpetrator from complying with such duty.

In addition to the penalties provided for in the DPA, an order can be made to temporarily or permanently prohibit the processing of data; publish the judgment or provide a public warning or censure of the controller.

Article 9 of Law 42 notes that the CNPD has authority to engage in legal proceedings and places a duty on it to report any criminal offences to the Public Prosecution Service.

Criminal offences

Article 35 notes that if the same violation is considered both a crime and an offence then the offender must be punished according to the crime. Furthermore, the penalties applied to concurrent offences are always materially accumulated.

Attempts to commit the crimes detailed below are punished by the same penalties.

In addition to the fines and penalties detailed in the table below, a temporary or permanent prohibition of processing, blocking, erasure or total or partial destruction of data may be ordered, in addition to the publication of a judgement or a public warning or censure of the controller. In the case of publication, it is done at the expense of the offender and is published in the periodical with the largest circulation in the area of the district where the infringement was committed, or in a periodical in the nearest district, and by means of affixing a notice for a period of no less than 30 days.

Civil remedies

Anyone who has suffered damage as a result of unlawful processing, is entitled to receive compensation from the controller. The right to receive compensation also extends to damage caused by any other act which is incompatible with "legal provisions in the area of personal data protection". The DPA does not explicitly limit this scope to infringements of provisions of the DPA. It is a defence for the controller to prove that she was not completely or partly responsible.

Administrative fines

The President of the CNPD is responsible for the fines detailed below, subject to prior deliberation by the Commission.

Offence	Category	Consequence
Failing to comply with notification obligations, providing false information or continuing to allow access to open data transmission networks to controllers who fail to comply with the provisions of the Law after being notified by the CNPD	Administrative	By an individual, a fine of between CVE 50,000 and CVE 500,000; By a group or entity, a fine of between CVE 300,000 and CVE 3,000,000; When referring to sensitive personal data per Article 24, the maximum fine is doubled
Failing to nominate a representative in Cabo Verde if not established on the territory, but using processing equipment in the territory. The same applies to negligence or attempt.	Administrative	A fine of between CVE 100,000 and CVE 1,000,000
Failure to comply with conditions on data quality in Article 6, such as processing for designated purposes, keeping data accurate, and storing for the allowed time period. The same applies to negligence or attempt	Administrative	A fine of between CVE 100,000 and CVE 1,000,000
Failure to honour a data subject's right to information about data being processed that relates to them. The same applies to negligence or attempt	Administrative	A fine of between CVE 100,000 and CVE 1,000,000
Failure to honour a data subject's right of access to data being processed that relates to them. The same applies to negligence or attempt	Administrative	A fine of between CVE 100,000 and CVE 1,000,000

Failure to honour a data subject's right to object to data being processed that relates to them. The same applies to negligence or attempt	Administrative	A fine of between CVE 100,000 and CVE 1,000,000
Failure to comply with Article 14's specification about non-subjection to automated individual decisions. The same applies to negligence or attempt	Administrative	A fine of between CVE 100,000 and CVE 1,000,000
Failure to comply with security precautions mandated by Article 16 for sensitive personal information. The same applies to negligence or attempt	Administrative	A fine of between CVE 100,000 and CVE 1,000,000
Processing data outside of instruction from the controller or legal requirements. The same applies to negligence or attempt	Administrative	A fine of between CVE 100,000 and CVE 1,000,000
Failure to make obligatory information available to a person who requests it from a controller. The same applies to negligence or attempt	Administrative	A fine of between CVE 100,000 and CVE 1,000,000
Failure to process data with consent or within the allowed criteria of Article 7. The same applies to negligence or attempt	Administrative	A fine of between CVE 100,000 and CVE 2,000,000
Violation of the provisions for the processing of sensitive personal data. The same applies to negligence or attempt	Administrative	A fine of between CVE 100,000 and CVE 2,000,000
Violation of the provisions regulating the processing of data relating to illegal activities, penalties, security measures, infringements, criminal and administrative offences, per Article 9. The same applies to negligence or attempt	Administrative	A fine of between CVE 100,000 and CVE 2,000,000
Violation of the provisions relating to the combination of data per Article 10. The same applies to negligence or attempt	Administrative	A fine of between CVE 100,000 and CVE 2,000,000

Violation of the provisions regulating the transfer of data to other countries. The same applies to negligence or attempt	Administrative	A fine of between CVE 100,000 and CVE 2,000,000
Intentionally failing to notify or apply for authorisation, providing false information, or making impermissible alterations to the information in the notifications or authorisations. The penalty is doubled for violations involving sensitive personal data or data relating to criminal and administrative offences	Criminal	Imprisonment of up to one year or a fine of up to 120 days[6]
Misappropriating or using personal data in a form incompatible with the purpose for which it was collected or with the legal instrument allowing its collection. The penalty is doubled for violations involving sensitive personal data or data relating to criminal and administrative offences	Criminal	Imprisonment of up to one year or a fine of up to 120 days
Carrying out an illegal combination of data. The penalty is doubled for violations involving sensitive personal data or data relating to criminal and administrative offences	Criminal	Imprisonment of up to one year or a fine of up to 120 days
Failure to comply with legal obligations within the time limit fixed by the CNPD for complying with them. The penalty is doubled for violations involving sensitive personal data or data relating to criminal and administrative offences	Criminal	Imprisonment of up to one year or a fine of up to 120 days
Continuing to allow access to open data transmission networks to controllers who fail to comply with the provisions of this Act after notification by the CNPD not to do so. The penalty is doubled for violations	Criminal	Imprisonment of up to one year or a fine of up to 120 days

[6] Note: both the English and Portuguese laws refer to a fine of up to 120 days.

involving sensitive personal data or data relating to criminal and administrative offences		
Gaining access by any means to data that is prohibited to that person. . The penalty is doubled when access is achieved by violating technical security rules, allowing a third party to obtain information, or providing a third party with a material advantage or benefit	Criminal	Imprisonment of up to one year or a fine of up to 120 days. Criminal proceedings are dependent on a complaint
Erasing, destroying, damaging, deleting, or changing personal data without authorisation, making them unusable or affecting their capacity for use	Criminal	Imprisonment of up to two years or a fine of up to 240 days. The penalty may be doubled if the damage caused is particularly serious. Up to one year imprisonment or a fine of up to 120 days in the case of negligence
Failure to cease processing after being notified, failing to collaborate with the CNPD after being notified, failing to destroy the personal data either totally or partially, or not destroying them after the allowed period for keeping them	Criminal	A penalty corresponding to the crime of qualified non-compliance
Violation of the duty of secrecy without due cause or consent. The penalty is increased by half if the agent is a civil servant, acts with the intention of obtaining a material advantage, or adversely affects the reputation, honour, and esteem or privacy of another person.	Criminal	Imprisonment for a period of between 6 months and 3 years or a fine of 80 to 200 days. Imprisonment of up to six months or a fine of up to 120 days for negligence. Criminal proceedings are dependent on a complaint except in the stipulated situations in which the penalty is increased by half

CÔTE D'IVOIRE

As at 11 September 2020

COUNTRY OVERVIEW			Ref
Is there a comprehensive data protection law?	☒	The Protection of Personal Information Act 2013-450.	Law link
Does the law establish a supervisory authority?	☒	The Law establishes the Protection Authority which sits within the Independent Administrative Authority in charge of Telecommunications Regulation and Information and Communication Technologies.	Article 46
Does the law define the term "personal information"?	☒	The term "personal data" is defined in Chapter 1 of the Laws.	Chapter 1
Does the law prohibit the processing of certain types of personal information?	☒	The Law prohibits the processing of certain types of personal information, subject to certain exceptions.	Article 21
Does the law prescribe its scope of application?	☒	The Law applies to both public and private bodies, as well as to both natural and juristic persons. Foreign entities, which are not domiciled in Côte d'Ivoire, must comply if they process data in the territory of Côte d'Ivoire.	Article 3
Does the law apply extra-territorially?	☐	No.	N/A
Does the law set out conditions for the lawful processing of personal information?	☒	The Law sets out at least eight conditions for the lawful processing of personal information.	Chapter 4 and Chapter 6
Does the law stipulate the requirements for valid consent?	☒	In order for consent to be valid, it must be express, unambiguous, free, specific and informed.	Article 1
Does the law require notification in the event of a data breach?	☐	No.	N/A
Can personal information be transferred to a third party in a foreign country?	☒	Personal information may be transferred provided the recipient country provides a similar level of protection.	Article 26
Does the law require a data protection impact assessment to be conducted?	☐	No.	N/A

Does the law require data processing registers?	☒	Yes.	Article 47
Does the law prescribe the use of terms of service icons?	☐	No.	N/A
Does the law prescribe penalties for non-compliance?	☒	The Law provides for criminal and administrative penalties for non-compliance.	Articles 21, 22, 45 and 51

LEGAL ANALYSIS

Legal framework

The Protection of Personal Information Act 2013-450 ('the Law') was enacted on 19 June 2013 to govern the protection of personal data.

Those responsible for processing personal data had a period of six months, from the date of entry into force of the Law, to comply with its provisions.

In addition to the Law, some aspects of personal data processing are regulated by decrees. For example, Article 13 states that the processing of personal data carried out on behalf of the State, or by a legal person governed by public law or private law managing a public service, is authorized by decree, following a reasoned opinion from the Protection Authority. This process relates to data processing regarding:

- State security, national defence or public security;
- Prevention, research, detection or prosecution of criminal offenses or the execution of criminal convictions or security measures;
- The population census;
- The treatment of salaries, pensions, taxes, and other settlements.

Decree No. 2015-79 of 4 February 2015 outlines the authorisation procedure for personal data processing. It sets the procedures for filing declarations, presenting requests and granting authorisations for the processing of personal data, as well as the terms for withdrawing authorisations and recovering financial penalties. The decree institutes fees for filing declarations and requesting authorisation for personal data processing.

Key definitions

In terms of the relevant role-players, the key definitions include the following:

- The term ***"data subject"*** is defined to mean any natural person who is the object of processing of personal data.

- The term ***"responsible party"*** is defined to mean the natural or juristic person, public or private, any other organization or association which, alone or jointly with others, takes the decision to collect and process personal data and determines its purposes.

- The term ***"subcontractor"*** is defined as any natural or legal person, public or private, or any other organization or association, that deals with data on behalf of the responsible party.

- The term ***"recipient of processing of personal data"*** is defined to mean any person authorized to receive communication of such data, other than the data subject, the data controller, the processor and the persons who, by reason of their functions, are responsible for processing the data.

The following definitions are also of relevance:

- The term ***"personal data"*** is defined to mean any information of any kind and regardless of its medium, including sound and image 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 their physical, physiological, genetic, psychological, cultural, social or economic identity.

- The term ***"processing of personal data"*** is defined to mean any operation or set of operations whether by automated or non-automated means, and applied to data, such as collection, operation, recording, organization, storage, adaptation, modification, extraction, saving, copying, consultation, use, communication by transmission, distribution or any other form of provision, reconciliation or interconnection, as well as locking, encryption, erasure or destruction of personal data.

- The term ***"identity"*** is defined to mean the postal or geographical address, telephone number and any other access number, information relating to location, billing or the location of communication equipment.

- The term ***"sensitive data"*** is defined to mean any data of a personal character that relates to opinions or activities of a religious, philosophical, political, trade union, sexual, racial, or health nature, or to social measures, prosecutions, penal or administrative sanctions.

- The term ***"Protection Authority"*** is defined to mean the independent administrative authority responsible for ensuring that the processing of personal data is implemented in accordance with the provisions of the Law.

- The term ***"consent of data subjects"*** is defined to mean any express, unambiguous, free, specific and informed manifestation of will by which the data subject, or their legal, judicial or contractual representative, accepts that their personal data may be processed manually or electronically.

- The term ***"third party country"*** is defined to mean any state that is not a member of the Economic Community of West African States (ECOWAS);

- The term ***"data linkage"*** is defined to mean any connection mechanism consisting of linking data processed for a specific purpose with other data processed for identical or different purposes, or linked by one or more data controllers.

The Law specifies that other terms not defined in the Law shall bear the meaning prescribed to them from ECOWAS, the AU or the ITU legal instruments.

Scope of application

Requirements for the scope of application

The following are subject to the provisions of the Law:

- Any collection, processing, transmission, storage and use of personal data by a natural person, the State, local authorities, or legal persons governed by public or private law;

- Any automated or non-automated processing of data contained or intended to appear in a file;

- Any data processing implemented on the national territory;

- Any processing of data relating to public security, defence, investigation and prosecution of criminal offences or the security of the State, subject to the exceptions defined by specific provisions laid down by other legal texts.

This raises the following considerations:

- ***Processing of personal information:*** there must be processing of personal information.

- ***Automated or non-automated means:*** it is irrelevant whether the responsible party makes use of automated or non-automated means.

- ***Implemented in Côte d'Ivoire***: the processing must be implemented in the national territory of Côte d'Ivoire.

What information does the law apply to?

The Law applies to the personal information relating to a natural person.

The Law does not restrict its application to Ivorian citizens. Rather, it protects the personal information of all data subjects in the country whose data is processed on its territory.

Compliance by responsible parties

Responsible parties are required to submit a declaration to the Protection Authority prior to processing personal data. The most common categories of data processing, particularly those which are not likely to infringe privacy or freedoms, may be exempted from prior declaration through the establishment and publication of standards and procedures by the Protection Authority. These are intended to simplify or exempt the controller from the obligation of prior declaration. Any processing done by the same body with a distinct purpose requires a separate declaration.

Responsible parties are also required to implement appropriate mechanisms to enable the right to be forgotten, the erasure of personal data and the periodic examination of the need to retain data.

The processing of data is confidential, and the Law has strict and detailed requirements for a responsible party to protect the security and integrity of the data and, in particular, to prevent distortion, damage, unauthorised access, and to prevent them from being used for the purposes of money laundering and financing of terrorism. Lastly, the responsible party is required to submit an annual report to the Protection Authority detailing their compliance with these requirements.

Compliance by operators

Article 20 states that when the processing of personal data is carried out on behalf of the responsible party, the latter must choose a subcontractor who provides sufficient guarantees for the protection and confidentiality of the data. It is incumbent on the responsible party and the subcontractor to ensure compliance with the provisions of the Law.

Exclusions

The Law provides for certain exclusions from its scope of application. These exclusions include the following:

- ***Personal or household activity***: data processing carried out by a natural person in the exclusive scope of his personal or domestic activities, provided that the data are not intended for systematic communication to third parties or for dissemination;

- ***Temporary copies:*** temporary copies made as part of the technical activities of transmission and provision of access to a digital network, with a view to the automatic, intermediate and transient storage of data and for the sole purpose of allowing other recipients of the service the best possible access to the information transmitted;

- ***Journalistic, research, literary or artistic purposes:*** processing of personal data for the purposes of journalism, research, or artistic or literary expression is permitted when it is implemented only for literary and artistic expression or for the exercise of activities of a journalist or researcher in a professional capacity, subject to the ethical rules of these professions.

Rights of data subjects

The Law sets out the following rights of data subjects:

- ***Notification:*** data subjects have a right to be notified by the responsible party of the identity of the responsible party, the purpose of the processing, the category of data concerned, the recipients to whom the data will be communicated and the possibility to refuse to appear on the file in question. They are further entitled to be notified of the existence of a right to access the data, the right to rectify these data; as well as the retention period of the data and any possibility of the data being transferred to a third country. Notification must be provided, at the latest, by collection

- ***Access:*** the right to know about the processing of their data, the right to confirmation that their data is or is not being processed by a responsible party, and the right to receive data that concerns them as well as any available information as to the origin of such data;

- ***Objection:*** the right to dispute the processing of their data, and to oppose its processing, in which case the responsible party may not process that data;

- ***Transfer:*** the right to be informed before data concerning them is communicated to third parties for the first time and to oppose, free of charge, said communication;

- ***Direct marketing:*** the right to be informed before data concerning them is used on behalf of third parties for marketing purposes and to oppose, free of charge, said use;

- ***Correction, destruction or deletion***: the right to demand the responsible party rectify, complete, update, lock or delete personal data concerning them which is inaccurate, incomplete, ambiguous or expired, or whose collection, use, disclosure or retention is prohibited. This right also applies to the descendants of a deceased person whose data they believe has not been updated. Data subjects also have the right to request the erasure and cessation of dissemination of data, particularly for data made available when they were a minor or if it is no longer necessary, if a person withdraws consent, the authorised storage period has expired, or any other legitimate reason.

Conditions for the lawful processing of personal information

The Law states that the collection, recording, processing, storage, transmission and interconnection of files of personal data must be done in a lawful and fair manner.

It requires responsible parties to submit a declaration to the Protection Authority prior to implementing the processing of personal data, except for the most common categories of data processing. The declaration (and requests for authorisation for special personal data) must contain certain information some of which includes: the purpose of the data processing, any linking of data that will be done, categories of people affected by the processing, who has access to the collected data, recipients authorised to receive communications about the data and, the precautions taken to ensure the confidentiality and security of the data.

Responsible parties must ensure they are in compliance with the following conditions:

- ***Prior declaration***: except in the circumstances provided for in the law;

- ***Consent***: the processing of personal data is considered legitimate only if the data subject has provided their express prior consent. Some exceptions to this requirement include: the receipt of authorisation or it is necessary for compliance with a legal obligation, for the performance of a mission of public interest or within the exercise of public authority, for the execution of a contract or pre-contractual measures or to protect the interests, rights and freedoms of the data subject;

- ***Purpose specification***: the data must be collected for an explicitly defined and legitimate purpose, and may not be processed in a manner incompatible with such purpose;

- ***Processing limitation***: the data must be adequate, relevant and not excessive in relation to the purpose for which it is collected and processed;

- ***Preservation period limitation***: the data must not be retained for longer than necessary to achieve the purposes for which it was collected and processed. Beyond this required period, the data may only be kept for historical, statistical or research purposes in accordance with legal provisions;

- ***Information quality:*** the data collected must be accurate and, if necessary, updated. All reasonable measures must be taken to ensure that inaccurate or incomplete data, with regard to the purposes for which they are collected and subsequently processed, are erased or rectified;

- ***Openness:*** the responsible party is obliged to provide clear information relating to personal data;

- ***Security safeguards:*** personal data must be treated in a confidential manner and protected, particularly when the processing of the data involves transmission on a network.

The following are not bound by the provisions on prior submission of declarations to the Protection Authority:

- ***Personal or household activity***: the processing of data used by a natural person within the exclusive framework of their personal, domestic activities or family. Similarly, the processing of data for the sole purpose of keeping a register which is intended for exclusively private use is also exempt;

- ***Public information:*** the processing of data concerning a natural person whose publication is prescribed by a legal provision or regulatory;

- ***Designated protection correspondent***: processing for which the responsible party has designated a correspondent for the protection of personal data who is responsible for independently ensuring the Law is complied with, except when a transfer of personal data destined for a third country is considered. This person must have the relevant qualifications required for exercising this mission, and must maintain a list of processing activities carried out that is immediately accessible to all on request. They cannot be subject to any sanction by the employer for actions taken in the course of their duties and can refer any difficulties they experience in the performance of their duties to the Protection Authority. This person's appointment must be reported to the Protection Authority and brought to the attention of employee representative bodies, where appropriate. In the event of a breach in duties by the correspondent, they are discharged of their duties on request, or after consultation with the Protection Authority.

Restrictions on the processing of personal information

Special personal information

The following types of personal data require pre-approval from the Protection Authority:

- Personal data relating to genetic, medical and scientific research in these areas;
- Personal data relating to offences, convictions or security measures pronounced by the courts;
- Personal data relating to a national identification number or any other identifier of the same nature, in particular telephone numbers;

- Personal data comprising biometric data;
- The processing of personal data for public interest purposes, particularly for historical, statistical or scientific purposes;
- The planned transfer of personal data to a third country.

The following types of data are prohibited from all collection and processing: data that reveal the racial, ethnic or regional origin, affiliation, political opinions, religious or philosophical convictions, trade union membership, sex life, genetic data or more generally those relating to the state of health of the data subject. The Law provides for some exceptions from this prohibition:

- ***Publicly available***: when the processing concerns data clearly made public by the data subject;

- ***Safeguard interests:*** when the processing of genetic data or data relating to health status is necessary to safeguard the vital interests of the data subject or of another person in the case that the data subject is physically or legally incapable of giving consent;

- ***Exercise of a legal right:*** when the processing, in particular of genetic data, is necessary for the establishment, exercise or defence of a legal right of the data subject;

- ***Legal proceedings:*** when legal proceedings or a criminal investigation are open. In this case, the processing of personal data is only allowed for the establishment of facts or for the manifestation of the truth;

- ***Specific organisation:*** when processing is carried out within the legitimate framework of a foundation, association or any other non-profit organization with political, philosophical, religious, mutualist or union purposes. However, the processing should relate only to members of that organisation or to persons maintaining regular contacts with it related to its purpose, and the data must not be communicated to third parties without the consent of the data subjects.

Children

The Law makes no specific mention of regulations relating to children.

Direct marketing

The Law prohibits direct marketing with the aid of any mode of communication using, in any form, the personal data of a natural person who has not expressly provided prior consent to receive such direct marketing.

Data subjects also have the right to oppose the processing of data relating to them for marketing purposes.

Automated decision-making

The Law stipulates that no court decision involving an assessment of the behaviour of a natural person may be based on automatic processing of personal data intended to assess certain aspects of his personality, while no administrative or private decision involving an assessment of the behaviour of a natural person may be based solely on automatic processing.

Data linkage

The linkage of data is only allowed to achieve the legal or statutory objectives of legitimate interest to the responsible party, and must receive prior authorisation from the Protection Authority. It cannot lead to discrimination or reduction of the rights, freedoms and guarantees for the data subjects, and appropriate security measures must be taken that take into account the relevance of the data being linked.

Transborder data transfers

The responsible party can only be authorised to transfer personal data to a third country – defined as countries outside ECOWAS - if this state ensures a higher or equivalent level of protection for privacy, freedoms and fundamental rights of individuals with regard to the processing of personal data. Before any transfer of personal data, the responsible party must first obtain the authorisation of the Protection Authority. The Protection Authority exercises oversight over the purpose of such transfers.

According to Decree 2015-79, requests for authorisation of the transborder transfer of personal data must be submitted to the Protection Authority by a juristic person bound by Ivorian law and must contain the following:

- Recent criminal records of the company's corporate officers;
- Motive and purpose of the transfer;
- Guarantees to protect the rights of data subjects;
- Explanation of the legal framework relating to personal data applicable in the country being transferred to;
- The means of transmission;
- Guarantees that the data subject and Ivorian authorities will have adequate access to the data to exercise their rights and powers.

The Decree also mandates that responsible parties submit an annual report to the Protection Authority detailing the activities of any transborder transfer of data to third countries.

Requirements for consent

Consent is defined in the Law to mean any express, unambiguous, free, specific and informed manifestation of will by which the data subject, or their legal, judicial or contractual representative, accepts that their personal data may be processed manually or electronically.

Transparency

Openness

Article 18 mandates the responsible party to provide clear information relating to personal data. The Article does not specify which information or in what form.

The Protection Authority is mandated by Decree 2015-79 to publish all decisions to withdraw authorisations given previously on their website.
Up to 80% of the amount received in fines is to be transferred to the public treasury.

Notification of a data breach

The Law does not make mention of notification procedures in the case of a data breach.

Impact assessments

The Law does not make mention of Impact Assessments.

Data processing registers

Article 47 of the Law mandates the Protection Authority to update a directory of personal data processing and make it available to the public for consultation.

Terms of service icons

The Law does not make mention of terms of service icons.

Additional transparency obligations

The Protection Authority is also required to submit an annual activity report to the President of the Republic and the President of the National Assembly, which may serve as an additional transparency mechanism.

Participation

Data subject participation

Article 30 of the Law details the rights of natural persons with regard to the access, rectification and deletion of data relating to them, including:

- ***Notification:*** the right to be notified by the responsible party, at the latest during collection, of the details concerning the collection of data;
- ***Access:*** the right to know about the processing of their data and to receive the data that concerns them as well as any available information as to the origin of such data;
- ***Objection:*** the right to dispute the processing of their data, and to oppose its processing;
- ***Transfer:*** the right to be informed before data concerning them is communicated to third parties for the first time and to oppose, free of charge, said communication;

- ***Direct marketing:*** the right to be informed before data concerning them is used on behalf of third parties for marketing purposes and to oppose, free of charge, said use;

- ***Correction, destruction or deletion***: the right to demand the responsible party rectify, complete, update, lock or delete personal data concerning them which is inaccurate, incomplete, ambiguous or expired, or whose collection, use, disclosure or retention is prohibited.

In cases where the responsible party fails in these duties, the Law provides mechanisms that empower the Protection Authority to step in to provide accountability.

Policy participation

Article 47 of the Law empowers the Protection Authority to determine the essential guarantees and measures appropriate for the protection of personal data, to give its opinion on any draft legal text in relation to the protection of freedoms and privacy, and to develop rules of conduct relating to the processing and protection of personal data. It also has the power to authorise certain conditions fixed by decree in the Council of Ministers on cross-border personal data transfers and to make proposals likely to simplify and improve the legislative and regulatory framework relating to the processing of personal data. Lastly, it is tasked with setting up mechanisms for cooperation with data protection authorities in other countries and participating in international negotiations on the protection of personal data.

Enforcement

Supervisory authority

The mandates of the Personal Data Protection Authority are entrusted to the Independent Administrative Authority in charge of Telecommunications Regulation and Information and Communication Technologies. The Protection Authority ensures that the processing of personal data is carried out in accordance with the provisions of the Law and its implementing decrees and ensures that the use of ICT does not infringe or pose a threat to freedoms and privacy for users in Côte d'Ivoire. Some of its responsibilities include:

- To **impose administrative and pecuniary sanctions** with regard to responsible parties who do not comply with the Law, or to withdraw authorisation previously granted;
- To **receive declarations and grant authorisations** for the implementation of the processing of personal data, or withdraw them;
- To **inform** data subjects and responsible parties of their rights and obligations;
- To **respond to** any request for advice on the processing of personal data;
- To **establish internal regulations** which specify the rules relating to the deliberation, investigation and presentation of files;

- To **receive claims and complaints** relating to the processing of personal data and inform others of the follow-up granted to them;
- To carry out, by means of sworn agents, **verifications** relating to any processing of personal data;
- To **update a directory** of personal data processing and make it available to the public for consultation;
- To **issue warnings** to responsible parties who do not comply with the Law, and formal notices to cease breaches within a specified time period.

The Protection Authority is also empowered to undertake an adversarial procedure in the case of a violation of rights and freedoms to cease the data processing activities, either temporarily or permanently. It also has the right to withdraw authorisations for processing either provisionally or definitively and issue financial penalties which are proportional to the seriousness of the breach and the benefits derived from it, not exceeding 10,000,000 CFA francs.

In cases where a data subject is unable to exercise their right of access through a responsible party, the Data Protection Authority has the power to investigate the matter and order the rectification, the deletion or blocking of data if processing does not comply with the Law.

The Supervisory Authority determines the appropriate period that personal data may be kept for, depending on the particular purpose it is being collected for and the types of processing.

Finally, the Protection Authority is required to submit an annual activity report to the President of the Republic and the President of the National Assembly.

Criminal offences

The Law provides for several criminal offences, such as the processing of prohibited types of personal data, direct marketing without consent, obstructing the work of the Protection Authority and failing to comply with warnings issued by the Authority, all of which are punishable by imprisonment and fines.

Civil remedies

The Law does not provide for civil remedies.

Administrative fines

The Law provides for administrative fines in cases where a responsible party does not respond to formal notices from the Protection Authority.

Offence	Category	Consequence
Processing of prohibited types of special personal data outside of the provisions of the Law	Criminal	Imprisonment of between 10 to 20 years and a fine of 20,000,000 to 40,000,000 francs CFA
Direct marketing using personal data without consent	Criminal	Imprisonment of between 1 to 5 years and a fine of 1,000,000 to 10,000,000 francs CFA
Hindering the action of the Protection Authority by refusing to hand over information or documents or misleading them	Criminal	Imprisonment of between 1 month to 2 years and a fine of 1,000,000 to 10,000,000 francs CFA
Failure to cease processing after formal notice from the Protection Authority	Administrative	A fine not exceeding 10,000,000 francs CFA
Continued failure to cease processing five years after receiving initial fine	Administrative	A fine not exceeding 100,000,000 francs CFA, or, in the case of a company, 5% of turnover excluding tax for the last financial year to a limit of 500,000,000 CFA francs

GHANA

As at 10 September 2020

COUNTRY OVERVIEW			Ref
Is there a comprehensive data protection law?	☒	Data Protection Act, 2012 (Act 843) (DPA).	Law link
Does the law establish a supervisory authority?	☒	The DPA establishes the Data Protection Commission.	S1(1)
Does the law define the term "personal information"?	☒	The terms "personal data" and "data" are defined.	S96
Does the law prohibit the processing of certain types of personal information?	☒	As a general principle, the DPA prohibits the processing of certain types of personal information, referred to as "special personal information" which includes the personal data relating to children and information concerning religious and political affiliation. This is subject to certain exceptions such as the provision of consent or that it is necessary for compliance with a legal obligation.	S37
Does the law prescribe its scope of application?	☒	The DPA applies to juristic persons and natural persons. If the Juristic person is not established in Ghana then it applies if they use equipment or a processor established in Ghana and if the data is not simply forwarded through Ghana.	S45
Does the law apply extra-territorially?	☒	The DPA applies to information which originates partly or wholly in Ghana, which may be interpreted as applying extra-territorially.	S45(1)(c)
Does the law set out conditions for the lawful processing of personal information?	☒	The DPA prescribes eight principles which must be applied when processing data.	S17
Does the law stipulate the requirements for valid consent?	☐	The DPA empowers the Minister to make regulations which specify the conditions that must be satisfied for consent to be given.	S94
Does the law require opt-in consent?	☐	No.	N/A

Does the law require notification in the event of a data breach?	☒	In the event of a data breach of personal data, the Data Protection Commission and the affected data subjects must be notified as soon as reasonably possible.	S31
Can personal information be transferred to a third party in a foreign country?	☐	There is no provision which expressly prohibits this.	S45(1)(c)
Does the law require a data protection impact assessment to be conducted?	☐	No.	N/A
Does the law require data processing registers?	☒	Yes.	N/A
Does the law prescribe the use of terms of service icons or an equivalent measure to inform consent of data use?	☐	No.	N/A
Does the law prescribe penalties for non-compliance?	☒	The DPA provides for criminal and civil penalties for non-compliance.	S95

LEGAL ANALYSIS

Legal framework

The Data Protection Act 843, 2012 (DPA) was enacted to protect the privacy of the individual by regulating the processing of personal information.

The DPA was assented to in May 2012 and came into force on 16 October 2012. Registration of Data Controllers and Data Processors started on 1 January 2015.

The DPA empowers the Minister to draft regulations concerning important content such as the requirements for consent and the prescription of additional safeguards. If the Regulations have been drafted, they are not easily accessible to the public.

Key definitions

The definitions are set out in section 96 of the DPA; some of the key definitions include the following:

- The term "***data subject***" means an individual who is the subject of personal data.

- The term "***data controller***" means a person who either alone, jointly with other persons, or as a statutory duty determines the purposes for and the manner in which personal data is processed.

- The term "***data processor"*** means any person, other than an employee of the data controller, who processes the data on behalf of the data controller.

- The term **"data"** means information which

  (a) is processed by means of equipment operating automatically in response to instructions given for that purpose;
  (b) is recorded with the intention that it should be processed by means of such equipment;
  (c) is recorded as part of a filing system, or with the intention that it would form part thereof;
  (d) forms part of an accessible record.

- The term "***personal data***" means "data about an individual who can be identified,

(a) From the data, or
(b) From the data or other information in the possession of, or likely to come into the possession of the data controller.

- The term "***processing***" is defined to mean:

  "an operation or activity or set of operations by automatic or other means that concerns data or personal data and the
  (a) collection, organisation, adaptation or alteration of the information or data;
  (b) retrieval, consultation or use of the information or data,
  (c) disclosure of the information or data by transmission, dissemination or other means available, or
  (d) alignment, combination, blocking, erasure or destruction of the information or data."

Scope of application

Requirements for the scope of application

The DPA applies to a data controller in the following circumstances:

- the data controller is established in Ghana and the data is processed in Ghana;
- the data controller is not established in Ghana but the data is processed by equipment or a data processor which is in Ghana;
- processing is in respect of information which originates partly or wholly from Ghana;

The DPA does not apply to data which originates externally and simply transits through Ghana.

The following data controllers are considered to be **established in Ghana**:

- Individuals who are ordinarily resident in Ghana;
- A body incorporated under the laws of Ghana;
- A partnership, persons registered under the Registration of Business Names Act, 1962 (Act 151) and the Trustees (Incorporation) Act, 1962 (Act 106);
- An unincorporated joint venture or association which operates completely or partly in Ghana;
- Any person who doesn't fall into the categories above but has an office, branch or agency which carries out business activities in Ghana.

The DPA also applies to the state and treats each government department as a data controller. Section 18(1) notes that if personal data originates from a foreign country, then it must be processed in accordance with the legislation of the foreign jurisdiction; the law is silent on what applies if the foreign country does not have data protection legislation.

What information does the law apply to?

Interestingly, the DPA does not include an explicit list of what kind of personal information the law applies to. It broadly defines 'personal data' as the information which could identify an individual.

An individual is not defined in the DPA so it is unclear whether it includes the personal information relating to juristic persons, but it seems from the wording that the information concerning juristic persons is not included.

Compliance by data controllers

All individuals who are ordinarily resident in Ghana must comply with the DPA, as well as companies, partnerships and trusts incorporated under the laws of Ghana. It also applies to companies which are established outside of Ghana but use equipment or a data processor within Ghana to process the information and to data controllers who process information which originates partly or wholly in Ghana. The DPA has a broad catch-all provision which brings any person who carries on business within Ghana within the ambit of the DPA - 'business' is defined to include trade or profession.

Importantly, every government department is considered a data controller.

Compliance by data processors

The DPA also applies to data processors which is any person, other than an employee of the data controller, who processes personal data on behalf of the data controller. They may only process personal data with the prior knowledge or authorisation of the data controller, must treat all information as confidential and may only disclose the data if required by law or for the discharge of a duty.

The DPA further stipulates that the processing of the personal data by a data processor must be governed by a written contract which requires the data processor to establish security measures in order to ensure the integrity of the personal data. If a data subject is not domiciled in Ghana, then the data controller must ensure that they comply with the relevant laws in Ghana.

Exclusions

The DPA provides for several exemptions from its scope of application. The exemptions include the following:

- ***National Security:*** processing of personal data is exempt from complying with the DPA for the purposes of public order; public safety; public morality; national security or public interest.

- ***Crime and Taxation:*** processing of personal data is exempt from complying with the DPA for the purposes of the prevention or detection of crime; the apprehension or prosecution of an offender; or the assessment or collection of a tax or duty.

- ***Health, education and social work:*** personal data which relates to the physical, mental health or mental condition of the data subject or personal data of an educational institution which relates to a pupil shall not be disclosed except if required by law.

- ***Regulatory activity:*** the provisions of the DPA do not apply to the processing of personal data for the protection of members of the public against loss or malpractice in the provision of banking, insurance, investment, financial services or management of a body corporate. It also doesn't apply when used against dishonesty of malpractice in professional services or to secure the health, safety and welfare of persona at work.

- ***Journalism, literature and art:*** a persona shall not process personal data unless it is for the publication of a literary or artistic material; it is in the public interest and the data controller reasonably believes that compliance with the DPA is incompatible with the special purposes. Despite this, the data controller must still comply with the provisions which relate to lawful processing; minimality; further processing; information quality and security safeguards.

- ***Research, history and statistics:*** the further processing of personal data for research purposes is not regarded as incompatible with the purpose for which the data was obtained, and it may be kept indefinitely. Personal data which is only processed for research purposes is exempt from the DPA if it is processed in compliance with the relevant conditions and the results of the research are not made available in a form which identifies any data subjects.

- ***Required by law:*** personal data is exempt from the provisions relating to non-disclosure when required by a rule of law or order of court.

- ***Domestic purposes***: if personal data is only processed for personal, family or household affairs then it is exempt from the data protection principles.

- ***Armed forces***: personal data is exempt from the DPA if its application would likely prejudice the combat effectiveness of the armed forces of Ghana.

- ***Judicial appointments and honours***: when personal data is processed to assess suitability for judicial office or to confer a national honour, it is exempt from compliance with the DPA.

- ***Public service or ministerial appointment***: the DPA provides that the Minister may make regulations to prescribe the exemptions concerning the processing of personal data for employment by the government or appointments made by the President.

- ***Examination marks and scripts:*** personal data is exempt if it relates to examination marks or if it is recorded during an academic or professional examination.

- ***Professional privilege:*** personal data is exempt from the subject information provisions of the DPA if it consists of information which is subject to professional privilege.

Rights of data subjects

The DPA provides for the following rights:

- ***Notification:*** the right to be notified that their personal information is being processed by the data controller or by another person on behalf of the data controller.

- ***Access:*** the right to establish whether a data controller holds personal information about them including a description of the data, the purpose for processing the data as well as information regarding the recipients of the data.

- ***Correction, destruction or deletion:*** the right to request the correction, destruction, or deletion of their data.

- ***Prevention:*** the right to require the data controller to cease or not begin processing data which causes or is likely to cause damage or distress.

- ***Direct marketing:*** the right to prevent the processing of their data for direct marketing.

- ***Automated decision-making:*** the right not to be subject to a decision which is based solely on automated processing of their personal information, and to be notified when such a decision is made.

- ***Compensation:*** where an individual suffers damage or distress due to non-compliance with the DPA, they are entitled to compensation.

- ***Manual data***: the right to require a data controller to rectify, block, erase or destroy manual data which is inaccurate or incomplete; or to cease to hold exempt manual data in a manner which is incompatible with the purpose.

- ***Request assessment:*** a person who is affected by the processing of personal data may request the Data Protection Commission to assess whether the processing complies with the DPA.

Conditions for the lawful processing of personal information

The DPA prescribes eight principles which must be applied when processing personal data. These principles are explicitly noted in section 17 and detailed in subsequent sections. The principles require the following:

- ***Accountability:*** requires that a person who processes personal data takes into account the privacy of the individual by applying the data protection principles.

- ***Lawfulness of processing***: requires that the data controller must ensure the data is processed without infringing the privacy rights of the data subject and that it is processed in a lawful and reasonable manner.

- ***Purpose specification:*** this principle requires that data may only be processed if the purpose of doing so is necessary, relevant and not excessive. The purpose must be specific, explicitly defined, lawful and must relate to the function or activity of the person.

- ***Compatibility of further processing:*** this principle requires that the further processing of personal data should be compatible with the purpose for which it was collected.

- ***Information quality:*** requires that the data controller ensure that the data is complete, accurate, up to date and not misleading.

- ***Openness:*** requires that the data controller take the necessary steps to ensure the data subject is aware of the purpose for the collection of the data and is notified of any security compromise which affects their data.

- ***Security safeguards:*** requires that the data controller take the necessary steps to secure the integrity of personal data in the possession or control of a person by taking appropriate, reasonable technical and organisational measures to prevent loss, damage or unauthorized access. In so doing, the data controller must identify foreseeable risks and regularly verify the effectiveness of the safety measures.

- ***Data subject participation:*** this principle requires that the data controller obtain the prior consent of the data subject before processing their data. It further provides that a data subject may request a data controller to confirm whether they hold their data and to provide a description of the data.

Restrictions on the processing of personal information

Special personal information

The DPA prohibits the processing of special personal information, subject to certain exceptions. Special personal information includes personal data which relates to a child who is under parental control and data which relates to the religious or philosophical beliefs, ethnic origin, race, trade union membership, political opinions, health, sexual life or criminal behaviour of an individual.

The prohibition on the processing of special personal information does not apply if one or more of the following exceptions is applicable:

- The processing is necessary;
- The data subject consents to the processing;
- The processing is necessary for the exercise or performance of a right or obligation conferred by law or by an employer;
- It is necessary for the protection of the vital interests of the data subject;
- It is carried out for the protection of the legitimate activities of a body or association.

The processing is presumed to be necessary if it is required for legal proceedings, for the establishment or defence of a right, in the course of the administration of justice or for medical purposes.

The DPA notes that the Minister may prescribe further conditions for the maintenance of appropriate safeguards for the rights and freedoms of a data subject related to the processing of special personal information.

Direct marketing

The DPA prohibits a data controller from using, obtaining, procuring or providing information related to a data subject for direct marketing purposes without the prior consent of the data subject. Direct marketing is defined to mean the communication by whatever means of any advertising or marketing material which is directed to particular individuals.

A data subject may write to a data controller at any time to request the data controller not to process their personal data for the purposes of direct marketing.

Automated decision-making

At any time, an individual may write to a data controller to request that any decision taken by or on behalf of the data controller, which significantly affects them, is not based solely on processing by automatic needs.

The DPA provides that a data controller must notify an individual where a decision has been made that is based solely on processing by automatic means. The data subject is entitled to request the data controller to reconsider the decision within twenty-one days and the data controller must notify them of the steps they have taken in this regard. This process does not apply to the following decisions:

- Those made in the course of considering whether to enter into a contract;
- In the performance of a contract;

- For a purpose required or authorised by an enactment;
- In other circumstances prescribed by the Minister.

Transborder data transfers

Interestingly, the DPA does not explicitly prohibit or regulate transborder data transfers. Section 45(1)(c) notes that the DPA applies to information which originates partly or wholly in Ghana, this could be read to mean that the DPA applies to such data regardless of where its processing takes place, and accordingly if it is transferred the DPA would still apply.

S47(1)(f) notes that in an application for registration as a data controller, the applicant must specify the name or description of the country to which the data may be transferred.

Requirements for consent

The DPA prescribes that personal data should not be processed without the prior consent of the data subject unless certain exceptions apply. The Minister is authorised to make regulations which specify the conditions for consent; these regulations are not publicly accessible if they have been drafted.

The legislative framework does not expressly prohibit discrimination for declining consent.

Transparency

Openness

Section 17(f) recognizes openness as one of the eight principles which protect privacy and must be applied when data is processed. This requires that if personal data is collected, the data controller must take the necessary steps to ensure that the data subject is aware of the purpose for the collection. Section 31(1) read with section 35(1) provides data subjects with a right to request access to their data. If requested, the data controller must confirm whether they hold data about the data subject, provide a description of the data and advise which third parties have access to it. They must further provide information concerning the source of the data.

The DPA stipulates that if a data controller is unable to comply with the request without disclosing the data related to another individual then they must not comply with the request unless certain conditions are met. These include consent from the other data subject or if it is reasonable to do so in the circumstances.

Notification of a data breach

A data controller is obliged to notify the Commission and affected data subjects when there are reasonable grounds to believe that their data has been accessed or acquired by an unauthorised person. The data controller must provide such notice as soon as reasonably possible after the discovery of the compromise.

The DPA specifies that if known, the data controller must disclose the identity of the unauthorised person who gained access to the data. The Commission may direct the data controller to publicise the data compromise.

Impact assessments

The DPA does not require data controllers to complete an impact assessment.

Data processing registers

The DPA establishes the Data Protection Register, which includes information concerning data controllers, and is maintained by the Commission. Upon applying for registration as a data controller, applicants must furnish specified information which includes their particulars, a description of the personal data they process, the purpose for doing so, a description of recipients of the data, countries to which the data may be transferred and a general description of their security measures. If insufficient information is supplied, then the Commission may refuse to grant an application.

A data controller may not process personal data unless they have been registered.

The DPA requires that the Commission provide facilities to make the information contained in the Register available for inspection by the public. Upon payment of a prescribed fee, the Commission must supply a member of the public with particulars from the register.

Terms of service icons

The DPA does not require the use of terms of service icons.

Additional transparency obligations

In addition to the above, the following measures may also serve to enhance transparency:

- ***Proactive disclosure****:* section 27 places an obligation on data controllers who intend to collect personal data to ensure that the data subject is aware of the nature of the data; the contact information of the data controller; the purpose for its collection; whether or not supplying the data is mandatory or voluntary; the consequences for failure to provide the data and the existence of their right to access such data and rectify it.

- ***Credit bureau as data controller****:* a request for information by a data subject is subject to the Credit Reporting Act and the DPA. Such a response must include the rights of a data subject under the Credit Reporting Act.

- ***Access to Information***: section 34 notes that the provisions of any legislation relating to the right to information are additional to the data subjects rights under the DPA

Participation

Data subject participation

Section 17(h) recognises data subject participation as one of the eight principles which must be taken into account when data is processed. The DPA provides for the following:

- ***Access to personal information:*** A data subject has the right to request a data controller to confirm whether or not they hold personal information about the data subject, and to request the data controller to provide a description of such personal information and to disclose its source.

- ***Request assessment:*** a person who is affected by the processing of their data may request the Data Protection Commission to assess whether such processing complies with the DPA.

- ***Correction or deletion of personal data:*** A data subject may request a data controller to correct or delete personal data about the data subject held by or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.

- ***Destruction or deletion of a record:*** A data subject may request a data controller to destroy or delete a record of personal data about the data subject that the data controller is no longer authorised to retain.

On receipt of a request to correct or delete personal information or to destroy or delete a record, the data controller must comply or provide credible evidence in support of the data. Where agreement cannot be reached between the data controller and the data subject, and if requested

to do so by the data subject, the data controller must attach to the record an indication that a request was made but not complied with. Where the request was complied with, the data controller must inform each person who received such information.

Policy participation

The Minister may give directives to the Board, which is the governing body of the Commission, on matters of policy.

Supervisory authority

The DPA establishes the Data Protection Commission (the Commission). Its object is to protect the privacy of the individual and personal data by regulating the processing of personal information and to provide the process to obtain, hold, use or disclose personal information.

The Data Protection Commission is empowered to implement and monitor compliance with the DPA; make appropriate administrative arrangements for the discharge of its duties; investigate and determine complaints and keep and maintain the Data Protection Register. It is further responsible for the provision of public education concerning the rights of data subjects and the obligations of data controllers.

Where the Data Protection Commission is satisfied that a data controller has contravened any of the data protection principles they may serve them with an enforcement notice. In such a notice, the Data Protection Commission can specify steps they must comply with or prohibit them from processing personal data as specified. Failure to comply with such a notice is an offence.

Criminal offences

Certain criminal offences are created under the DPA. Some of these include knowingly supplying false information in support of an application for registration as a data controller; processing personal data without registering as a data controller and selling or offering to sell personal data of another person. The penalties for contravention include a fine and/or imprisonment of up to 5 years, while others carry a penalty of a fine and/or imprisonment of up to 1 year.

Civil remedies

The DPA provides that where an individual suffers damage or distress through the contravention by a data controller of the requirements of the Act, that individual is entitled to compensation from the data controller. There are no thresholds stipulated in the DPA required for the institution of such compensation. It specifies that defence to such a claim would include evidence that reasonable care was taken to comply.
The DPA does not expressly provide for class action proceedings.

Administrative fines

The DPA does not use the term 'administrative fine' and only refers to those included in criminal proceedings.

Offence	Category	Consequence
Knowingly supplying false information in support of an application for registration as a data controller	Criminal	A fine of not more than 150 penalty units or imprisonment not exceeding 1 year, or both
Processing personal data without registering as a data controller	Criminal	A fine of not more than 250 penalty units or imprisonment not exceeding 2 years, or both
Failure to comply with an enforcement notice	Criminal	A fine of not more than 150 penalty units or imprisonment not exceeding 1 year, or both
To knowingly make a false statement when complying with an information notice	Criminal	A fine of not more than 150 penalty units or imprisonment not exceeding 1 year, or both
Recklessly making a statement which is false in a material sense in complying with an information notice	Criminal	A fine of not more than 150 penalty units or imprisonment not exceeding 1 year, or both
A person who provides goods, facilities or services to the public and requires the supply or production of a particular record as a condition for their provision	Criminal	A fine of not more than 250 penalty units or imprisonment not exceeding 2 years, or both
An employee or agent of the Data Protection Commission knowingly or recklessly discloses information	Criminal	A fine of not more than 2 500 penalty units or imprisonment not exceeding 5 years, or both
Purchasing personal data or information contained in the personal data of another person	Criminal	A fine of not more than 250 penalty units or imprisonment not exceeding 2 years, or both
Knowingly obtaining or knowingly or recklessly disclosing the personal data or the information contained in the personal data of another person	Criminal	A fine of not more than 250 penalty units or imprisonment not exceeding 2 years, or both
Disclosing or causing to be disclosed to another person the information contained in personal data	Criminal	A fine of not more than 250 penalty units or imprisonment not exceeding 2 years, or both

Selling or offering to sell personal data of another person	Criminal	A fine of not more than 2 500 penalty units or imprisonment not exceeding 5 years, or both
Committing an offence under the Regulations	Criminal	A fine of not more than 5 000 penalty units
Contravention by a data controller of the requirements of the DPA which causes damage or distress to an individual	Civil	Compensation

KENYA

As at 16 September 2020

COUNTRY OVERVIEW			Ref
Is there a comprehensive data protection law?	☒	The Data Protection Act, 2019 (the DPA)	Law link
Does the law establish a supervisory authority?	☒	Yes, the Office of the Data Protection Commissioner.	S5
Does the law define the term "personal information"?	☒	The terms "personal data" and "data" are defined in section 2 of the DPA but they do not include a list of the types of information included.	S2
Does the law prohibit the processing of certain types of personal information?	☒	As a general principle, the DPA prohibits the processing of certain types of personal information, referred to as "sensitive personal information", as well as the personal information of children. This is subject to certain exceptions such as the provision of consent or that it is necessary for the defence of a legal claim.	S44
Does the law prescribe its scope of application?	☒	The DPA applies to natural and legal persons and public authorities. Foreign entities, which are not established in Kenya, must comply if they process personal data of data subjects located in Kenya.	S4
Does the law apply extra-territorially?	☒	The DPA applies to data controllers which are not established or resident in Kenya but who process the personal data of data subjects located in Kenya.	S4(b)(ii)
Does the law set out conditions for the lawful processing of personal information?	☒	Yes, the DPA sets out eight conditions and obligations.	S25
Does the law stipulate the requirements for valid consent?	☒	Yes, it must be express, unequivocal, free, specific and informed.	S2; S32
Does the law require opt-in consent?	☒	The DPA requires a clear affirmative action or an indication of the data subject's agreement.	S2

Does the law require notification in the event of a data breach?	☒	In the event of a data breach of personal data, the Data Commissioner must be informed within 72 hours and the affected data subjects must be notified as soon as reasonably possible.	S43
Can personal information be transferred to a third party in a foreign country?	☐	As a general principle, the DPA prohibits the transfer of personal data to a third party in a foreign country. This is subject to certain exceptions.	S48
Does the law require a data protection impact assessment to be conducted?	☒	Yes.	S31
Does the law require data processing registers?	☒	Yes.	S21
Does the law prescribe the use of terms of service icons or an equivalent measure to inform consent of data use?	☐	No.	N/A
Does the law prescribe penalties for non-compliance?	☒	The DPA provides for criminal, civil and administrative penalties for non-compliance.	S56 - 66

LEGAL ANALYSIS

Legal framework

The Data Protection Act, 2019 (DPA)was enacted to regulate the processing of personal data to protect the privacy of individuals. The object of the DPA further notes the establishment of institutional mechanisms and the provision of rights and remedies.

The DPA commenced on 25 November 2019.

In addition to the DPA, the Cabinet Secretary is empowered to make regulations in order to give effect to the DPA. Section 71 notes that such regulations may concern processing requirements; the levying of fees; measures to safeguard data subjects' rights or any other matter. To date, no regulations have been published or are not readily available to the public.

Key definitions

The DPA applies to the processing of personal data of a data subject, which has been entered into a record by or for a data controller or processor.

The definitions are set out in section 1 of the DPA. In terms of the relevant role-players, the key definitions include the following:

- The term "***data subject***" means an identified or identifiable natural person who is the subject of personal data.

- The term "***data controller***" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing personal data.

- The term "***data processor***" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

The following definitions are also of relevance:

- The term "**data"** means:
  "information which –
  (a) Is processed by means of equipment operating automatically in response to instructions given for that purpose;
  (b) Is recorded with the intention that it should be processed by means of such equipment;
  (c) Is recorded as part of a relevant filing system;

(d) Where it does not fall under paragraph (a) (b) or (c), forms part of an accessible record; or
(e) Is recorded information which is held by a public entity and does not fall within any paragraphs (a) to (d).”

- The term “***personal data***” is defined to mean: any information relating to an identified or identifiable natural person.

- The term “***processing***” is defined to mean:

  “any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means such as -
  (a) collection, recording, organisation, structuring;
  (b) storage, adaptation or alteration;
  (c) retrieval, consultation or use;
  (d) disclosure by transmission, dissemination, or otherwise making available; or
  (e) alignment or combination, restriction, erasure or destruction.”

- Despite forming an important part of the definition, the term “record” is not defined in the DPA.

Scope of application

Requirements for the scope of application

The DPA applies to “the processing of personal data entered in a record, by or for a data controller or processor, by making use of automated or non -automated means: Provided that when the recorded personal data is processed by non-automated means, it forms a whole or part of a filing system; by a data controller or data processor who (i) is established or ordinarily resident in Kenya and processes personal data while in Kenya; or (ii) not established or ordinarily resident in Kenya, but processing personal data of data subjects located in Kenya.” Accordingly, in order for the DPA to apply, the following elements are required:

- ***Processing of personal information:*** there must be processing of personal information.

- ***Entry into a record:*** the personal data must be entered into a record by or for a data controller or processor.

- ***Automated or non-automated means:*** it is irrelevant whether the data controller makes use of automated or non-automated means. Automated means is not defined in the DPA. If the personal data is processed by non-automated means, it must form part of a filing system.

- ***The data controller or processor:*** the DPA applies if the data controller or processor is established or a resident in Kenya and processes personal data in Kenya. It also applies to controllers and processors which aren't established or resident in Kenya, but process the personal data of data subjects located in Kenya.

What information does the law apply to?

The DPA applies to the personal data relating to an identifiable natural person. It does not apply to the data concerning juristic persons.

The DPA does not restrict its scope of application to Kenyan citizens. Section 4(b)(ii) requires data controllers and processors which are not established or resident in Kenya to process the personal data of data subjects *located in Kenya*. This limits its scope by not including the data of Kenyan data subjects living outside of Kenya but does not exclude data subjects in Kenya that are not citizens. This limitation does not apply to data controllers or data processors that are established or resident in Kenya and it is accordingly unclear whether this section broadens its scope to include data concerning Kenyans who are not located in Kenya. The law does not include a condition that the data partly or wholly originated in Kenya.

Compliance by data controllers

All natural and legal persons who process personal data must comply with the DPA. This includes members of the public, public authorities, agencies and other bodies. The 'other bodies' are not defined or specified in the DPA.

Compliance by data processors

The DPA also applies to data processors which process personal data on behalf of the data controller. This includes natural and legal persons, public authorities, agencies and other bodies.

Importantly, the DPA requires that both the data controller and the data processor register with the Data Protection Commissioner.

Exclusions

Part VII of the DPA deals with exemptions and notes that nothing in this part shall exempt any data controller or processor from complying with data protection principles relating to lawful processing, minimisation, data quality and the adoption of security safeguards.

The following exemptions are provided for in the DPA:

- ***Personal or household activity:*** processing of personal data in the course of a purely personal or household activity.

- ***National security***: processing is necessary for national security or public interest. The DPA does not specify what constitutes 'national security' or 'public interest'.

- ***Required by law:*** disclosure is required by written law or by court order.

- ***literary or artistic purposes:*** the processing is undertaken for the publication of literary or artistic material, and the data controller reasonably believes that it is in the public interest and compliance with the provisions is incompatible with the purpose. The description of this section is noted as 'Journalism, literature and art', however there is no mention of journalism under this exemption. The inclusion of journalism may be intimated from section 52(2) which requires compliance with a code of ethics which ordinarily regulates journalism. The Data Commissioner is obligated to prepare a code of practice to guide the processing of personal data for Journalism, Literature and Art.

- ***Research, History and Statistics:*** further processing for historical, statistical or research purposes is considered compatible with the purpose of collection. Personal data which is processed only for research is exempt from the DPA if it is processed in compliance with the conditions and the results are published in a form which does not identify data subjects.

The Data Commissioner is empowered to prescribe further instances which may be exempt.

Rights of data subjects

The DPA sets out the following rights of data subjects, which include the following:

- ***Informed:*** the right to be informed about how their data will be used;

- ***Access:*** the right to access their personal data in the custody of the data controller or processor;

- ***Objection:*** the right to object to the processing of all or part of their personal information. The data controller or processor may continue to process the data if they can demonstrate a compelling interest to do so or for the establishment, exercise or defence of a legal claim;

- ***Correction:*** the right to correct false or misleading data;

- ***Deletion***: the right to delete false or misleading data;

- ***Withdraw consent:*** section 32(2) empowers a data subject to withdraw consent at any time, unless otherwise provided in the DPA;

- ***Automated decision-making:*** section 35(1) provides the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or significantly impacts the data subject.

- ***Data portability***: a data subject has a right to receive their personal data in a structured, common, machine-readable format, and the right to transmit it to another data controller or processor. This right does not apply where processing is necessary for a task in the public interest or in the exercise of official authority.

Interestingly, section 27 of the DPA notes the circumstances under which such rights may be exercised by someone other than the data subject. This includes where the data subject is a minor or has a mental disability. It also allows the right to be exercised by any other person duly authorised by the data subject.

Conditions for the lawful processing of personal information

The DPA prescribes that every data controller or data processor must comply with eight principles and obligations which include:

(a) processing must be in accordance with the data subject's right to privacy;

(b) personal data must be processed lawfully, fairly and in a transparent manner;

(c) personal data must be collected for explicit, specified and legitimate purposes and not further processed in a way which is incompatible with that purpose;

(d) personal data must be adequate, relevant and limited to what is necessary for the purpose;

(e) Collected only where a valid explanation is provided whenever information relating to family or private affairs is required;

(f) Accurate and kept up to date which includes an obligation to take reasonable steps to ensure that inaccurate data is corrected or erased;

(g) Kept in a form which identifies the data subjects for no longer than is necessary;

(h) Not transferred outside of Kenya unless there is proof of adequate safeguards or consent from the data subject.

Section 28(1) requires that personal data be collected directly from the data subject unless it is contained in a public record; it has been made public by the data subject; the data subject consents; it is necessary for the prevention, investigation or prosecution of a crime; necessary for the enforcement of a law or the protection of the interests of the data subject.

Section 39(2) places a limitation on the processing of personal data by requiring that it shall only be retained for as long as reasonably necessary. This is subject to exemptions, which include the consent of the data subject, authorization by law; necessary for a lawful purpose or for historical, statistical, journalistic, literature, art or research purposes. At the expiry of the retention period, the data controller must delete, anonymize or pseudonymize personal data.

Restrictions on the processing of personal information

Sensitive personal information

The DPA prohibits the processing of sensitive personal data, subject to certain exceptions. Sensitive personal data is defined, in section 2, to include: a natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents or spouse, sex or the sexual orientation of the data subject.

The DPA is authorised to prescribe further categories of personal data which may be classified as sensitive personal data.

The prohibition on the processing of special personal data does not apply if one or more of the following exceptions is applicable:

- ***Not for profit body*:** the processing is carried out during the course of the activities of a foundation, association or not for profit body which has a political, philosophical, religious or trade union aim. It is further required that the processing concerns its members, and the data is not disclosed outside of the body without consent.

- ***Public:*** the personal data has been made public by the data subject;

- ***Necessary:*** the processing is necessary for the establishment, exercise or defence of a legal claim; or for the obligations or rights of the data controller or data subject or necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent.

Children

The DPA prohibits the processing of personal data concerning a child, subject to certain exceptions. A 'child' is not defined in the DPA.

The prohibition does not apply if consent is provided by the child's parent or guardian and it is processed in a manner which protects and advances the rights and best interests of the child. Such consent is not required if the processing is done exclusively for the provision of counselling or child protection services.

Data controllers and processors are required to utilise appropriate mechanisms to verify age and consent in order to process a child's personal data. These mechanisms must be determined based on available technology; the volume of data; the proportion of data likely to concern a child and the possibility of harm to a child caused by the processing.

Direct marketing

The DPA prohibits the use of personal data of a data subject for commercial purposes, subject to certain exceptions. The term "direct marketing" is not used (beyond the index) or defined, instead, the DPA broadly refers to commercial purposes.

The prohibition on the processing of personal data for commercial purposes does not apply if one or more of the following exceptions is applicable:

- ***Consent:*** the data subject has given his or her express consent to the processing.

- ***Authorised by law:*** it is authorised by any written law and the data subject has been informed of such use when the data was collected.

The DPA requires that when using the data for such purposes it must be anonymised where possible to ensure that the data subject is no longer identifiable.

Automated decision-making

The DPA provides that a data subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or significantly affects the data subject.

The prohibition on automated decision-making does not apply if one or more of the following exceptions is applicable:

- ***Contract:*** it is necessary for entry into or performance of a contract between the data subject and the data controller;

- ***Authorised by law:*** the data controller is authorised to do so by law, and such law includes suitable safeguards for the data subject's rights and interests.

- ***Consent:*** the data subject consents to it;

If such a decision is taken, the data subject must be notified and may request the data controller or processor to reconsider the decision or make a decision that is not based solely on automated processing. The data controller must comply and notify the data subject of the steps which have been taken as well as the outcome. The Cabinet Secretary is empowered to make regulations which provide additional safeguards for a data subject's rights, freedoms and interests concerning automated decision making.

Transborder data transfers

The DPA prohibits the transborder transfer of personal data. One of the principles in section 25 obliges data controllers and data processors to ensure that personal data is not transferred outside of Kenya without proof of adequate safeguards for data protection, or consent from the data subject. The Data Commissioner may request a demonstration of the appropriate safeguards and may prohibit, suspend or impose conditions on such a transfer.

The prohibition on transborder data transfers does not apply if one or more of the following exceptions is applicable:

- ***Appropriate safeguards***: the data controller or processor has provided proof to the Data Commissioner of appropriate safeguards concerning the security and protection of the personal data.

- ***Commensurate laws***: the data controller or processor has provided proof to the Data Commissioner of appropriate safeguards including jurisdictions with commensurate data protection laws.

- ***Necessary***: the transfer is necessary for:
  (a) the performance of a contract between the data subject and the data controller;
  (b) a contract concluded between the data controller and a third party in the interests of the data subject;
  (c) any matter of public interest;

(d) The establishment, exercise or defence of a legal claim;
(e) To protect the vital interests of the data subject and the data subject is incapable of providing consent;
(f) For the pursuit of legitimate interests of the data controller which are not overridden by the interests, rights and freedoms of the data subject.

Sensitive personal data may only be transferred out of Kenya with the consent of the data subject and upon confirmation of appropriate safeguards.

Requirements for consent

Consent is defined in section 2 to mean:

"any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject."

The DPA prescribes that a data controller or data processor bears the burden of proof for a data subject's consent. It allows the data subject to withdraw consent at any time and notes that such withdrawal will not affect the lawfulness of previous processing.

In determining whether consent was freely given the DPA considers whether the performance of a contract or service is conditional on the provision of consent to the processing of additional, unnecessary personal data. It intimates that other things must be taken into account, but these are not specified.

The legislative framework does not expressly prohibit discrimination for declining consent.

Transparency

Openness

The principles of data protection, outlined in section 25, includes a requirement that personal data is processed in a transparent manner.

Before collecting personal data, there is an obligation on data controllers and data processors, to inform the data subject that their information is being collected; its purpose; the third parties to whom it will be transferred, relevant contact details; security measures in place; their rights, and the consequence of failing to provide the requested data.

Notification of a data breach

A data controller is obliged to provide notification when personal data has been accessed or acquired by an unauthorised person and there is a real risk of harm to the data subject. The data controller must notify the Data Commissioner within 72 hours of becoming aware of the breach and must notify the data subject within a reasonably practical period. The data controller may delay notifying the data subject if it is necessary for the prevention, detection or investigation of an offence.

A data processor is obligated to notify the data controller of a breach within 48 hours of becoming aware of it.

Section 43(6) provides that a data controller does not have to notify the data subject of a breach if the data controller or processor has implemented appropriate security safeguards which may include encryption of the affected data.

Impact assessments

The DPA requires that a data protection impact assessment must be conducted where a processing operation is likely to result in high risk to the rights and freedoms of a data subject. High risk is not defined but the provision notes that it must be determined based on its nature, scope, context and purpose, and the Data Commissioner must set out guidelines for the assessment. The assessment report must be submitted to the Data Commissioner sixty days before processing.

The impact assessment must include the following:

- A description of the processing and the interest of the data controller or processors;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- A risk assessment concerning the rights and freedoms of the data subject;
- The safeguards and mechanisms which will be in place to protect the personal data and demonstrate compliance with the DPA.

Data processing registers

Section 18 of the DPA prohibits data controllers and processors from acting unless registered with the Data Commissioner. The Data Commissioner is required to prescribe the thresholds for mandatory registration and the DPA specifies the considerations which must be taken into account when doing so. Registration entails an application process and the provision of information including a description of the personal data, the purpose for it, risks and safeguards and any other details prescribed by the Data Commissioner.

The register is a public document and is available for inspection by any person. A request may be made to the Data Commissioner for a certified copy of any entry.

The Data Commissioner may cancel the registration or vary the conditions of the certificate of registration. It may do so if any information provided by the applicant is false or misleading, or they fail to comply with any requirement of the DPA. It may also conduct periodical audits of the processes and systems of data controllers or processors to ensure compliance with the DPA.

Terms of service icons

The DPA does not require the use of terms of service icons.

Participation

Data subject participation

The principles which must be considered during the processing of personal information do not explicitly include data subject participation. However, the participation of a data subjects is provided for throughout the DPA, and includes the following:

- ***Access to personal information:*** the DPA provides data subjects with a right to access their personal data which is in the custody of a data controllers and processors.

- ***Request restriction:*** data subjects may request that the processing of their data be restricted if they contest its accuracy, it is no longer required for the purpose or its processing is unlawful. When under such a restriction, the data may only be processed with the data subject's consent, for the defence of a legal claim or for the protection of rights. The data subject must be informed if the restriction is withdrawn.

- ***Rectify:*** a data subject may request a data controller or processor to rectify personal information about the data subject in its possession or under its control that is inaccurate, out of date, incomplete or misleading.

- ***Erasure or destruction:*** a data subject may request a data controller to erase or destroy personal data that is irrelevant, excessive, obtained unlawfully or which the data controller is no longer authorised to retain.

Where the data has been shared with a third party, the data controller or processor must take reasonable steps to inform them of the request for rectification, erasure or destruction. If such data is required for the purpose of evidence, the data subject must be informed of that.

Policy participation

The DPA does not specifically refer to policy participation but the Data Commissioner is required to research developments in data processing to minimise risk.

Enforcement

Supervisory authority

The DPA establishes the Office of the Data Protection Commissioner (the Data Commissioner). The provisions note that it is designated as a State Office in terms of Article 260 (q) of the Constitution, and lists its capacity as an entity which includes the ability to sue and be sued as well as to enter into contracts.

The Data Commissioner is responsible for overseeing the implementation and enforcement of the DPA; it must establish and maintain the register of data controllers and processors and promote self-regulation. It must further promote international cooperation relating to data protection and conduct research into new developments in order to mitigate risk. Section 5(4) places an obligation on the Data Commissioner to ensure reasonable access to its services in all parts of Kenya.

The DPA includes several provisions in section 8, concerning the oversight and enforcement functions of the Data Commissioner. First, it provides that the Data Commissioner must exercise oversight of data processing operations, which it may do on its initiative (referred to as its own motion) or at the request of a data subject – this includes verifying whether processing complies with the DPA. Second, it may conduct an assessment of a public or private body, also on its initiative or following a request from a public or private body, to determine if data is being processed in terms of the DPA. Third, it may carry out inspections of public and private entities to evaluate the processing of personal data. Fourth, it may receive and investigate any complaint by any person concerning the infringement of rights. This raises the following considerations:

- It is difficult to discern any distinction between these functions, all of which entail assessing compliance with the DPA. The first appears to be a catch-all provision for oversight, while the second is narrowed to public or private bodies. The purpose of restricting that function to public and private bodies is unclear – particularly because the terms are not defined, and scarcely used throughout the DPA.
- Interestingly, the duty to 'investigate' appears to be limited to complaints concerning the infringement of rights.

In light of the above it is important to read the functions of the Data Commissioner with its powers which are outlined in section 9. These include the power to:

- Conduct investigations on its initiative or following a complaint made by a data subject or a third party;
- Facilitate conciliation, mediation and negotiation on disputes concerning the DPA;
- Issue summons to a witness for the purposes of investigation;
- Require any person to provide explanations or information;
- Impose administrative fines for failure to comply with the DPA;

Section 23 – which deals with data processing registers – notes that the Data Commissioner may carry out periodical audits of the processes and systems of data controllers to ensure compliance with the DPA.

Section 57 notes that for an investigation of a complaint, the Data Commissioner may order any person to attend an oral examination; produce a document or furnish a statement under oath. This section does not explicitly note the Data Commissioner's power to subpoena, but does state that failure to comply and the provision of false or misleading information is an offence.

Where the Data Commissioner is satisfied that a person has failed to comply with the DPA, an enforcement notice may be served on them which specifies the steps which must be taken to remedy the situation. Failure to comply with such a notice is an offence.

The Data Commissioner is authorised to seek assistance from a person or authority for the gathering of information or an investigation. The Data Commissioner is further empowered to obtain a warrant from a Court and then enter and search any premises.

Data Protection Officers

It is not mandatory to appoint a data protection officer. Section 24(1) notes that a data controller or processor *may* do so where the processing is carried out by a public or private body, the nature of the processing requires systematic monitoring of data subjects or they process sensitive data. If one is appointed, their contact details must be published on their website and published by the Data Commissioner. The data protection officer must ensure compliance with the DPA, facilitate capacity building and co-operate with the Data Commissioner.

Criminal offences

Certain criminal offences are created under the DPA. These include the failure or refusal to comply with an enforcement notice, the provision of false or misleading information and disclosure of personal data to a third party. Certain contraventions carry a penalty of a fine of up to five million shillings and/or imprisonment of up to 10 years, or both.

Civil remedies

The DPA makes provision for a person who suffers damage due to a contravention of the DPA to claim compensation from the data controller or processor. A data controller will be liable for any damage caused by processing. A data processor will only be liable for damage caused by processing if they did not comply with a provision in the DPA aimed specifically at data processors, and they have acted contrary to their lawful instructions.

Damage includes financial loss and distress. The DPA does not specify the burden of proof or the threshold of fault.

Administrative fines

If the Data Commissioner is satisfied that a person is failing to comply with a provision of the DPA, it may issue a penalty notice which requires the payment of a specified fine. The DPA notes the factors which must be considered when determining whether to issue such a notice and the amount payable. These factors include:

(a) the nature and gravity of the failure;
(b) whether it is negligent or intentional;
(c) any action taken to mitigate the damage;
(d) the degree of fault present;
(e) previous failures;
(f) the degree of co-operation with the Data Commissioner to remedy the failure;
(g) categories of data effected;
(h) the way in which the infringement became known to the Data Commissioner;
(i) the extent of compliance with previous enforcement notices and penalty notices;
(j) adherence to approved codes of conduct;
(k) any aggravating or mitigating circumstances;
(l) whether the penalty would be effective, proportionate and dissuasive.

The maximum fine which may be imposed by the Data Commissioner is five million shillings, or one per cent of annual turnover of the previous financial year, whichever is lower.

Any administrative action taken by the Data Commissioner may be appealed in the High Court.

Offence	Category	Consequence
Failure or refusal to comply with an enforcement notice	**Criminal**	A fine not exceeding five million shillings or imprisonment for a term not exceeding two years, or both
Obstructs or impedes the Data Commissioner in the exercise of their powers.	**Criminal**	A fine not exceeding five million shillings or imprisonment for a term not exceeding two years, or both.
Failure to provide assistance or information requested by the Data Commissioner	**Criminal**	A fine not exceeding five million shillings or imprisonment for a term not exceeding two years, or both
Refusing to allow the Data Commissioner to enter any premises or to take any person with them in the exercise of their functions	**Criminal**	A fine not exceeding five million shillings or imprisonment for a term not exceeding two years, or both
Provision of false or misleading information in any material aspect	**Criminal**	A fine not exceeding five million shillings or imprisonment for a term not exceeding two years, or both
Unlawful disclosure of personal data which is incompatible with its purpose for collection	**Criminal**	A fine not exceeding three million shillings or imprisonment for a term not exceeding ten years, or both
A data processor discloses personal data without the prior authorisation of the data controller	**Criminal**	A fine not exceeding three million shillings or imprisonment for a term not exceeding ten years, or both
Disclosure of personal data to a third party	**Criminal**	A fine not exceeding three million shillings or imprisonment for a term not exceeding ten years, or both
Offering to sell personal data which was unlawfully disclosed	**Criminal**	A fine not exceeding three million shillings or imprisonment for a term not exceeding ten years, or both
A data controller causes damage through processing	**Civil**	Damages for financial loss and distress
A data processor causes damage due to non-compliance with a provision in the DPA which specifically applies to data processors and acted in contravention of lawful instruction	**Civil**	Damages for financial loss and distress
Failure to comply with the DPA	**Administrative**	A fine of up to five million shillings, or one per cent of annual turnover of the previous financial year, whichever is lower

LIBERIA

As at 23 September 2020

Liberia has no comprehensive data protection legislation.

In 2010, Liberia signed the Supplementary Act on Personal Data Protection. The Act appears to be strongly influenced by the EU Data Protection Directive (95/46/EC) from 1995 and is legally binding. It requires signatory states to establish a legal framework for the protection of privacy of data and sets out the required formalities for executing personal data processing, such as prior declaration and authorization for certain types of processing. It also specifies that each member state will establish a Data Protection Authority. Liberia has yet to establish such a framework.

In 2018, Liberia's Ministry of Post and Telecommunications validated a new 5-year Telecommunications and ICT Policy, which aims to "ensure the expansion of ICT infrastructure across the country, the development of e-Government services and applications, the provision of universal access to voice and internet services in isolated communities." Despite this, there have been no public utterances of the intention to implement data protection legislation.

MALAWI

As at 29 September 2020

COUNTRY OVERVIEW			Ref
Is there a comprehensive data protection law?	☒	No, but some data protection provisions are included in the Electronic Transactions and Cyber Security Act, 2016.	Cybersecurity Act
Does the law establish a supervisory authority?	☐	The Cybersecurity Act notes that the Malawi Communications Regulatory Authority is responsible for the implementation of the Act, and the Malawi Computer Emergency Response Team is established to respond to information and communication technology security threats. Their capacity to enforce compliance with the Act in terms of data protection is unclear.	S5 and S6
Does the law define the term "personal information"?	☒	The term "personal data" is defined in the Cybersecurity Act.	S2
Does the law prohibit the processing of certain types of personal information?	☐	No.	N/A
Does the law prescribe its scope of application?	☐	The Cybersecurity Act does not prescribe its scope of application in terms of the data protection provisions.	N/A
Does the law apply extra-territorially?	☐	No.	N/A
Does the law set out conditions for the lawful processing of personal information?	☒	Yes, the Cybersecurity Act notes six conditions for the lawful processing of personal data.	S71
Does the law stipulate the requirements for valid consent?	☒	Yes, consent must be freely given, specific and informed.	S71(3)
Does the law require opt-in consent?	☐	No.	N/A
Does the law require notification in the event of a data breach?	☐	No.	N/A

Can personal information be transferred to a third party in a foreign country?	☐	The Cybersecurity Act does not deal with transborder transfers of personal data.	N/A
Does the law require a data protection impact assessment to be conducted?	☐	No.	N/A
Does the law require data processing registers?	☐	No.	N/A
Does the law prescribe the use of terms of service icons or an equivalent measure to inform consent of data use?	☐	No.	N/A
Does the law prescribe penalties for non-compliance?	☒	The Cybersecurity Act creates certain criminal offences concerning personal data but does not explicitly note that non-compliance with the data protection principles constitutes an offence.	S83

LEGAL ANALYSIS

Legal framework

Malawi does not have a consolidated and comprehensive law which governs data protection. However, part VII of the Electronic Transactions and Cybersecurity Act No. 33 of 2016 (the Cybersecurity Act) regulates some aspects of data protection and privacy. The Cybersecurity Act was promulgated on 4 November 2016.

Despite utterances in March 2018 by the Minister of Information and Communication Technology of the intention to enact a data protection law, no draft has been published.

Key definitions

The Cybersecurity Act includes several relevant definitions, including the following:

- The term ***"data subject"*** is defined as a person from whom data relating to that person is collected, processed or stored by a data controller.

- The term ***"data controller"*** means a person who, acting alone or with others, determines the purpose and manner in which personal data is processed and therefore controls and is responsible for the keeping and using of personal data. The definition specifically includes a person who collects, processes, or stores personal data.

- The term "***personal data"*** is defined to mean any information which relates to an individual who may be directly identified or may be identifiable by reference to an identification number or by one or several elements related to his physical, physiological, genetic, psychological, cultural, or economic identity.

- The term "***data"*** means the electronic presentation of information in any form. This definition appears to exclude manual data by its use of the term 'electronic'.

- The "***processing of data***" is defined to include "any operation or set of operations which is performed upon data, whether or not by automatic means such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Scope of application

Requirements for the scope of application

The Cybersecurity Act does not include a provision concerning the scope of application of the data protection provisions. It places obligations on data controllers, but the definition of a data controller does not include any detail on whether it applies to juristic and natural persons. It also does not specify whether it applies to data controllers outside of Malawi.

What information does the law apply to?

The Cybersecurity Act applies to information which can identify an individual. It is unclear whether this includes juristic persons. The definition of personal data specifically includes physical, physiological, genetic, psychological, cultural, and economic identity. However these elements are not further defined or clarified, and it is accordingly unclear what information would fall within, for example, an economic identity.

Compliance by data controllers

The Cybersecurity Act places an obligation on responsible parties to comply with the provisions for lawful processing and to notify data subjects of specified information. Section 74 requires that they implement technical and organisational measures to protect data against accidental or unlawful destruction, loss, alteration and unauthorised access and disclosure. Such measures must provide an appropriate level of security for the risks posed by the processing and nature of the data. It is further unclear whether state entities are bound by the Cybersecurity Act.

Compliance by operators

The Cybersecurity Act does not mention operators or extend the obligations to them.

Exclusions

The Cybersecurity Act does not provide for any exclusions.

Rights of data subjects

The Cybersecurity Act provides data subjects with the following three rights:

- ***Access and notification:*** this right entitles the data subject to obtain confirmation on whether their data is processed; to be notified of such processing including the source of the data, the purpose for its processing and to whom it will be disclosed;

- ***Objection:*** this right entitles a data subject to object to the processing of their personal information at any time based on legitimate grounds. The Cybersecurity Act does not outline the conditions which would constitute legitimate grounds. If the objection is justified, then the data controller may no longer process it.

- ***Correction, destruction or deletion:*** the data subject is entitled to request the rectification, erasure or blocking of their personal data if its processing does not comply with the provision of the Cybersecurity Act, particularly if it is incomplete or inaccurate.

Conditions for the lawful processing of personal information

The Cybersecurity Act prescribes that personal data must be processed in accordance with 6 conditions, which include:

- ***Lawful and fair:*** personal data must be processed fairly and legally;

- ***Purpose specification:*** personal data must be collected for a specified, explicit and legitimate purpose and may not be further processed in a manner incompatible with such purpose.

- ***Adequate:*** personal data must be adequate, relevant and not excessive in relation to its purpose.

- ***Information quality:*** personal data must be accurate and kept up to date.

- ***Erasure and rectification:*** every reasonable step must be taken to ensure that inaccurate and incomplete personal data is erased or rectified.

- ***Retention:*** personal data must not be retained in a form which allows for the identification of data subjects for longer than necessary.

The Cybersecurity Act further prescribes that personal data may only be processed for the following reasons:

- ***Consent***: the data subject has unambiguously provided consent;
- ***Contract performance:*** processing the data is necessary for the performance of a contract to which the data subject is party, or it has been requested by the data subject prior to entering into a contract;
- ***Legal obligation:*** the processing is necessary to comply with a legal obligation of the data subject;
- ***Vital interest:*** the processing is necessary to protect the vital interests of the data subject;

- ***Public interest:*** the processing is necessary for a task carried out in the public interest or in the exercise of official authority vested in a data controller or third party to whom the data is disclosed. Public interest is not defined or clarified further in the Cybersecurity Act and it is accordingly unclear what would constitute such a circumstance.
- ***Legitimate interests:*** processing is necessary for the legitimate interests of a data controller or third party who receives the data, except where such interests are overridden by the rights, interests and freedoms of the data subject.

Restrictions on the processing of personal information

Special personal information

The Cybersecurity Act does not define or regulate special personal data.

Children

The Cybersecurity Act does not mention the personal data of children.

Direct marketing

The Cybersecurity Act prohibits the dissemination of unsolicited electronic communications without consent. Unsolicited communications are not defined and it is accordingly unclear whether direct marketing falls within the scope of this prohibition included in section 42. Section 42(2) notes that when a person sends electronic commercial communication to a consumer, they must provide an option to unsubscribe and if requested, must provide the particulars of the source of the data.

Automated decision-making

The Cybersecurity Act does not refer to automated decision making.

Transborder data transfers

The Cybersecurity Act does not refer to transborder data transfers.

Requirements for consent

Consent is one of the justifications for the lawful processing of personal information. Consent is defined in section 71(3) to mean “any freely given specific and informed indication by a data subject, of his wishes, by agreement, to his personal data being collected, processed or stored.”

A data subject may withdraw consent at any time, provided that the withdrawal will not affect the lawfulness of the processing which occurred before the withdrawal of consent. The Cybersecurity Act does not specifically provide for a data subject's ability to withdraw consent nor does it expressly prohibit discrimination for declining consent.

Transparency

Section 73 places an obligation on data controllers to notify data subjects of the following information:

- The data controller's identity;
- The purposes for processing the data;
- The existence of the right to access and rectify their personal data;
- The existence of the right to object to the processing of their data.

Notification of a data breach

The Cybersecurity Act does not require notification following a data breach.

Impact assessments

The Cybersecurity Act does not require data controllers to complete a data impact assessment.

Data processing registers

The Cybersecurity Act does not require the creation or publication of a data processing register.

Terms of service icons

The Cybersecurity Act does not require the use of terms of service icons.

Additional transparency obligations

There are no additional transparency obligations provided by the Cybersecurity Act.

Participation

Data subject participation

The rights afforded to data subjects in the Cybersecurity Act concern data subject participation. These rights include their entitlement to access and be notified of the processing of their

personal data; the right to object to the processing of their information and the right to request correction, destruction or deletion of personal data.

Policy participation

The Cybersecurity Bill does not refer to policy participation in the context of data protection.

Enforcement

Supervisory authority

Section 5 of the Cybersecurity Act notes that the Malawi Communications Regulatory Authority is responsible for the implementation of the Act. This would invariably include implementation of the provisions concerning data protection, however it is not explicitly mandated to ensure compliance with these provisions.

Section 6 establishes the Malawi Computer Emergency Response Team (CERT). The Malawi CERT is mandated to respond to information and communication technology security threats. Again, it is also not specifically mandated to monitor and enforce compliance with the data protection provisions. It is accordingly unclear whether the Cybersecurity Act designates a supervisory authority for data protection or how the Regulatory Authority or Malawi CERT would extinguish these duties without prescribed powers.

Criminal offences

The Cybersecurity Act creates a few offences which apply to data, these include unauthorised access or destruction of data. However; some offences are unclear, and it is accordingly difficult to ascertain whether they apply to data protection. For example, section 83(6) of the Cybersecurity Act concerns the prohibition of the disclosure of information to unauthorized persons. It is not clear whether this section includes the disclosure of personal data because the term 'information' is not defined. Section 83(6)(a) and (b) creates an offence for the disclosure of information which was accessed pursuant to the powers provided under a search warrant. Because the Cybersecurity Act does not explicitly note that non-compliance with the data protection provisions constitutes an offence, it is unclear whether a warrant may be applied for in this context.

Criminal offences are detailed in section 84 of the Cybersecurity Act and carry a penalty of a fine of K 2 000 000 and imprisonment for five years. Section 84(1) notes that where an offence is committed which concerns data relating to national security or the provision of an essential service, then the penalty is imprisonment for a term of not less than ten years, but not exceeding fifteen years.

Civil remedies

The Cybersecurity Act does not explicitly provide for civil remedies concerning the data protection provisions.

Administrative fines

The Cybersecurity Act does not explicitly provide for administrative fines concerning the data protection provisions.

Offence	Category	Consequence
Intentionally accessing or intercepting any data without authority or permission	Criminal	A fine of K 2 000 000 and to imprisonment for five years
Intentionally and without authority interferes with data in a way which causes its modification, destruction or renders it ineffective	Criminal	A fine of K 2 000 000 and to imprisonment for five years
The unlawful production, selling, procurement, design, distribution or possession of any device which is designed to overcome security measures for the protection of data	Criminal	A fine of K 2 000 000 and to imprisonment for five years
The utilisation of a device designed to overcome security measures for the protection of data	Criminal	A fine of K 2 000 000 and to imprisonment for five years
Damaging, deleting, altering or suppressing data without authorisation	Criminal	A fine of K 2 000 000 and to imprisonment for five years
Knowingly receiving data which a person is not authorised to receive	Criminal	A fine of K 2 000 000 and to imprisonment for five years
Attempting to commit any of the listed offences	Criminal	A penalty not exceeding one half of the maximum penalty imposed by the provision creating the offence.
Aiding or abetting another person to commit an offence under the Cybersecurity Act	Criminal	A penalty imposable by the provision creating the offence.
Sending unsolicited commercial communications to another person or continuing to do so after the person has unsubscribed	Criminal	A fine of K 1 000 000 and to imprisonment for twelve months

MOROCCO

As at 15 September 2020

COUNTRY OVERVIEW			Ref
Is there a comprehensive data protection law?	☒	Law no. 09-08 of 18 February 2009.	Law link
Does the law establish a supervisory authority?	☒	The Law established the National Commission for the Control of the Protection of Personal Data (the CNDP).	Article 27
Does the law define the term "personal information"?	☒	The term "personal data" is defined in Article 1 of the Law.	Article 1
Does the law prohibit the processing of certain types of personal information?	☒	The Law does not generally prohibit the processing of sensitive personal data but provides requirements for its legal processing. Data relating to offences, convictions and security measures can only be processed by courts and their officials and other public authorities.	Articles 12, 21 and 24
Does the law prescribe its scope of application?	☒	The Law applies to both public and private bodies, as well as to both natural and juristic persons. Foreign entities, which are not domiciled in Morocco, must comply if they conduct activity in Morocco or do more than simply forward personal information through the country.	Article 2
Does the law apply extra-territorially?	☐	No.	N/A
Does the law set out conditions for the lawful processing of personal information?	☒	The Law sets out five conditions for the lawful processing of personal information.	Article 3
Does the law stipulate the requirements for valid consent?	☒	In order for consent to be valid, it must be free, specific and informed.	Article 10
Does the law require notification in the event of a data breach?	☐	No.	N/A

Can personal information be transferred to a third party in a foreign country?	☐	Data may be transferred to a foreign country subject to certain requirements, including prior authorisation.	Chapter V
Does the law require a data protection impact assessment to be conducted?	☐	No.	N/A
Does the law require data processing registers?	☐	No.	N/A
Does the law prescribe the use of terms of service icons?	☐	No.	N/A
Does the law prescribe penalties for non-compliance?	☒	The Law provides for criminal and administrative penalties for non-compliance.	Chapter VII

LEGAL ANALYSIS

Legal framework

Law no. 09-08 of 18 February 2009 ('the Law') was enacted to protect natural persons with regards to the processing of the personal data, which was promulgated on 18 February 2009. The law is available in French.

Entities and people who processed data prior to publication of the Law had two years from the date of installation of the CNDP - which would be published in the Official Bulletin – to ensure compliance.

In addition to the Law, the legal framework comprises Decree no. 2-09-165 of 21 May 2009 (the Decree). The Decree defines the methods and conditions for the nomination of members to the CNDP, as well as the rules and regulations for its functioning.

Key definitions

The Law applies to the processing of personal data concerning natural persons.

The definitions are set out in Article 1. In terms of the relevant role players, the key definitions include:

- The term ***"data subject"*** is defined to mean any natural person who can be identified or identifiable through personal data, directly or indirectly, in particular by reference to an identification number or to one or more specific elements of their physical, physiological, genetic, psychological, economic, cultural or social identity;

- The term ***"responsible party"*** is defined to mean the natural or juristic person, public authority, service or any other entity which, either alone or jointly with others, determines the purposes and means of processing personal data;

- The term ***"sub-contractor"*** is defined to mean the natural or juristic person, public authority, service or any other entity which processes personal data on behalf of the responsible party;

- The term ***"third party"*** is defined to mean the natural or juristic person, public authority, service or any other entity other than the data subject, the responsible party, the sub-contractor or any people who, under the direct authority of the responsible party or sub-contractor, are authorised to process the data;

- The term ***"recipient"*** is defined to mean the natural or juristic person, public authority, service or any other entity who receives communications of data, whether or not it is a third party, except for bodies who are likely to receive communication of data within the framework of a legal provision who are not considered recipients.

The following definitions are also of relevance:

- The term ***"personal data"*** is defined to mean all information, of whatsoever nature or medium including sound and images, that relates to an identified or identifiable natural person;

- The term ***"processing of personal data"*** (or ***"processing"***) is defined to mean any operation or set of operations carried out using either automated or non-automated processes and applied to personal data, such as collection, recording, organization, storage, adaptation or modification, extraction, consultation, use, communication by transmission, broadcast or any other form of provision, reconciliation or linkage, as well as blocking, erasure or destruction;

- The term ***"sensitive data"*** is defined to mean the personal data of a data subject that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or which is related to the subject's health, including genetic data;

- The term ***"consent by a data subject"*** is defined to mean any manifestation of will that is free, specific and informed, by which the data subject accepts that personal data concerning them will be subject to processing;

- The term ***"transfer or communication"*** is defined to mean any disclosure or informing of data brought to the attention of a person other than a data subject;

- The term ***"data linkage"*** is defined to mean a form of processing that consists of establishing a connection between data from a file and data from a file or multiple files held by another party or other parties, or held by the same responsible party but for another purpose;

Scope of application

Requirements for the scope of application

The Law applies to the processing of personal data that is either partially or wholly automated, as well as non-automated processing that is contained or intended to be contained in manual file records. This raises the following considerations:

- ***Processing of personal information:*** there must be processing of personal information;
- ***Entry into a record:*** the personal information must be entered into a record by or for a responsible party;
- ***Automated or non-automated means:*** it is irrelevant whether the responsible party makes use of automated or non-automated means;
- It is carried out by a ***natural or juristic person***;
- The responsible party is ***established on Moroccan territory***. Carrying out activities on Moroccan territory, regardless of legal form, is considered being established there. Therefore, responsible parties who use processing means that are located in Moroccan territory are also bound by the Law. Processing which is only used for purposes of transit through the territory or that of a State whose data protection legislation is recognised as equivalent to that of Morocco are excluded.

What information does the law apply to?

The Law applies only to information concerning identified or identifiable natural persons. It does not restrict its scope of application to Moroccan citizens; rather, it applies to any data processing occurring in the Moroccan territory.

Compliance by responsible parties

All natural and juristic persons must comply with the Law, subject to some explicit exclusions.

Legal processing of personal data requires prior declaration to the CNDP, if it is not subject to prior authorisation as detailed in the “Special personal information” section.

The declaration must include:

- The name and address of the responsible party or their representative;
- The description, characteristics and purpose of the intended processing;
- A description of the categories of data subjects and the related data;
- The recipients of the data;
- Any envisaged transfer of the data to foreign states;
- The retention period of the data;
- How the data subject may exercise their rights to access and notification;
- Measures taken to ensure the confidentiality and security of the data;
- Details of any crossovers, linkage, or any other form of reconciliation of data as well as their transfer or subcontracting in any form to third parties, whether free or for a fee.

Any changes to the above details must be reported to the CNDP.

According to Article 18, the prior declaration obligation does not apply to processing operations whose sole purpose is to keep a register which, by virtue of legislative or regulatory provisions, is intended for public information and open to the public, as defined by the CNDP. However, in this case, a data controller must be appointed, whose identity is made public and communicated to the CNDP. The data controller is responsible for the application of the provisions of the Law. The controller must communicate to any person who requests information relating to the name and purpose of the processing, the identity of the controller, the data processed, their recipients and, where applicable, any intended transfers.

The CNDP may decide to subject a declaration to the requirement for prior authorisation if it foresees that the envisaged processing poses manifest dangers to the protection of privacy and the fundamental rights and freedoms of the data subjects.

Responsible parties, as well as people who have knowledge of personal data processed in the performance of their duties, are required to respect professional secrecy even beyond the termination of the exercise of their functions.

Personal data may only be communicated to a third party for the achievement of purposes that are directly linked to the pre-defined purposes and subject to the prior consent of the data subject.

Compliance by operators

The responsible party is required to choose a sub-contractor which can provide sufficient guarantees of the technical and organisational measures required for the data processing and the responsible party must ensure compliance with these measures.

The performance of the subcontracting must be governed by a contract or a legal act which binds the subcontractor to the responsible party. It must state that the subcontractor acts under the sole instruction of the responsible party, and that the obligations of the responsible party are also incumbent on them.

Exclusions

The Law provides for certain exclusions from its scope of application, which include the following:

- ***Personal or household activity***: processing of personal data carried out by a natural person for the exercise of activities exclusively of a personal or domestic nature;

- ***National security:*** personal data collected or processed in the interest of national defence and internal or external state security. It also does not apply to data collected for the prevention and repression of crime other than under conditions fixed in law or regulation;

- ***Legislative implementation:*** personal data collected in application of specific legislation, which must be communicated to the CNDP;

Rights of data subjects

Article 5 of the Law prescribes the rights of data subjects concerning personal data related to them, which include the following:

- ***Notification:*** data subjects have the right to know the identity of the responsible party, the purpose for which their data is being collected, the recipients of the data, and the details of the declaration sent to or authorisation received from the CNDP. The right further entails notification on whether answering the questions is compulsory or optional along with the consequences of a default response, the existence of a right to access personal data that concerns them and to correct. This right does not apply to the following:

    - Data collected for national defence or state security purposes;
    - Data collected for the prevention or repression of crime;
    - When notification is impossible, notably for statistical, historical or scientific purposes, in which case the responsible party must notify the CNDP of this fact and provide a reason;

- When the law expressly provides for the registration or communication of personal data;
- Data processing carried out exclusively for journalistic, artistic or literary purposes.

- ***Access:*** data subjects have the right to receive free and timely confirmation from the responsible party that their data is being processed, as well as information relating to the purpose, the type of data, and the recipients of the data, and access to the data itself;

- ***Automated decision-making:*** data subjects have the right to know the logic behind any automated processing of personal data that concerns them;

- ***Correction, destruction or deletion:*** the data subject has the right to request that their personal data be updated, corrected, erased or blocked if the processing does not conform with the Law, notably by being incomplete or incorrect. This right also applies to third parties to whom the data has been communicated. In such cases, the responsible party must undertake the corrections at no cost to the applicant within ten days;

- ***Redress***: in the event that a responsible party refuses or does not respond to requests for correction, destruction or deletion of data within the defined period, the data subject may submit a request for correction to the CNDP, which will investigate and have the necessary corrections made as soon as possible, while keeping the data subject updated and informed.

- ***Objection:*** the data subject has the right to object to data concerning them being processed for legitimate reasons, as well as to object to data concerning them being used for marketing purposes, particularly commercial purposes. This does not apply when the processing is necessary for a legal obligation or is expressly authorised by law.

Conditions for the lawful processing of personal information

Article 3 of the Law prescribes numerous conditions for the lawful processing of personal data. It is the responsibility of the responsible party to ensure compliance with these conditions, which are as follows:

- ***Processing limitation:*** personal data must be processed fairly and lawfully, and only if it is adequate, relevant and not excessive relative to the purpose for which it was collected and ultimately processed;

- ***Purpose specification:*** personal data must be collected for a specific, explicitly defined, and legitimate purpose, and may not be treated in a manner incompatible with its purpose;

- ***Information quality:*** the personal data must be accurate and, if necessary, updated. All reasonable measures must be taken to erase or correct data that is inaccurate or incomplete with regard to the purpose for which it was collected and processed;

- ***Retention limitation***: personal data which may identify data subjects must only be kept for as long as necessary for the realisation of the purposes for which it was collected. On request by a responsible party, the CNDP may authorise the retention of data for historical, statistical, or scientific methods for longer periods of time;

- ***Security safeguards:*** appropriate technical and organisational measures must be taken to protect personal data against accidental or illegal destruction, accidental loss, alteration, distribution or unauthorised access. Article 24 of the Law outlines specific additional security precautions that must be taken when processing sensitive data or data relating to health.

Restrictions on the processing of personal information

Special personal information

Processing of personal data must be subject to a prior authorisation when it concerns:

- Sensitive data, defined as personal data that reveals the racial or ethnic origin, political opinions, religious or philosophical convictions, or trade union membership of a data subject or that concerns health, including genetic data;
- The use of personal data for purposes other than what it was collected for;
- Genetic data, except when it is used by health personnel for preventative or diagnostic medicine or medical care;
- Data relating to offences, convictions or security measures, except when implemented by court officials;
- Data including the number of the national identity card of the data subject;
- The linkage of files belonging to one or more juristic persons managing a public service and whose purposes are different, or the linkage of files belonging to different legal persons with different purposes;

The authorisation is granted if any of the following applies:

a) express consent from the data subjects;
b) the processing is essential for the exercise of the legal or statutory functions of the responsible party;
c) the processing is necessary to defend the vital interests of the data subject or a person and they are physically or legally unable to give consent;

d) the processing relates to data clearly made public by the data subject and their consent to the processing of data can legitimately be inferred from its statements; or if
e) the processing is necessary for the recognition, exercise or defence of a legal right and is carried out exclusively for this purpose.

Sensitive data

Processing of sensitive data is exempt from the requirement of prior authorisation when it is carried out by an association or any other non-profit group of a religious, philosophical, political, trade union, cultural or sporting nature. The data must only relate to members of the group or those who maintain regular contact with it, processing must correspond to the purpose of the group, and the data must not be communicated to third parties without consent.

Health data and selection

The processing of health data is exempt from pre-authorisation when it is related to preventative or diagnostic medicine, or health care administered by a health practitioner bound by professional secrecy. Processing does however require prior declaration. The same requirement applies to processing for the purpose of selecting the people likely to benefit from a right, a service or a contract.

Offences and security measures

The processing of personal data relating to offences, convictions and security measures can only be implemented by courts and their officials and other public authorities. Similarly, only public entities may create, maintain or process central registers relating to persons suspected of illicit activities, offences and administrative offences and decisions providing for penalties, security measures, fines and ancillary sanctions.

Children

The Law makes no specific mention of the processing of data related to children.

Direct marketing

The Law defines direct marketing as sending any message either directly or indirectly that is intended to promote goods, services or the brand of a person selling goods or providing services. The Law prohibits direct marketing by means of an automatic call machine, fax machine or electronic mail or in any way using the contact details of a natural person who has not expressed their prior consent to receive direct marketing.

Direct marketing by e-mail is allowed if the recipient's contact details have been collected directly from them, through a sale or provision of services, if the direct prospecting concerns similar products or services provided by the same natural or legal person. The recipient must be expressly, unambiguously and simply notified of the possibility of opposing the use of their contact details when they are collected and each time a prospecting email is sent to them.

Automated decision-making

No court decision involving an assessment of a person's behaviour may be based on automated processing of personal data intended to assess certain aspects of their personality. No other decision producing legal effects for a person may be taken on the sole basis of automated data processing intended to define the profile of the person concerned or to assess certain aspects of their personality.

Decisions taken in the context of the conclusion or performance of a contract and for which the data subject has been placed in a position to present their observations are not considered to be taken on the sole basis of automated processing, nor those satisfying the requests of the data subjects.

Transborder data transfers

A responsible party may not transfer personal data to a foreign state unless that state provides a sufficient level of protection for privacy and the fundamental rights and freedoms of people with regard to the processing of personal data. The CNDP draws up a list of states that meet this criteria.

Data may be transferred to a state that does not meet this requirement if the data subject has provided express consent or if the transfer is necessary for:

- The protection of the life of that person;
- For the preservation of the public interest;
- To ensure the establishment, exercise or defence of legal claims;
- For the execution of a contract between the responsible party and the data subject, or in fulfilment of precontractual measures taken at their request;
- For the conclusion or execution of a contract between the responsible party and a third party if it is in the interest of the data subject;
- The execution of a measure of international legal assistance;
- The prevention, diagnosis or treatment of medical conditions.

Alternatively, data may be transferred if it is for the implementation of a bilateral or multilateral agreement which Morocco is party to, or with authorisation of the CNDP when a sufficient level of protection for privacy and the fundamental rights and freedoms of individuals is guaranteed.

Requirements for consent

Processing of personal data may only be carried out if the data subject has undoubtedly given their consent to the operation or to all the operations envisaged. However, consent is not required if the processing is necessary for:

- Fulfilment of a legal obligation to which the data subject or the responsible party are subject;
- Execution of a contract to which the data subject is party, or for the execution of precontractual measures taken at their request;
- Safeguarding the vital interests of the data subject, if they are physically or legally unable to give their consent;
- Execution of a task of public interest or within the exercise of public authority which is vested in the responsible party or the third party to whom the data has been communicated;
- Realisation of a legitimate interest pursued by the responsible party or the recipient, without disregarding the interests, fundamental rights and freedoms of the data subjects.

Transparency

Openness

Articles 5 and 7 state that data subjects have the right to notification and access to data relating to them. In cases where a responsible party refuses access, the CNDP is empowered to step in to ensure data subjects are able to exercise these rights.

Notification of a data breach

The Law does not specify notification procedures to be taken in the case of a data breach. The CNDP is, however, endowed with investigative powers to determine whether any breaches of the Law have occurred.

Impact assessments

The Law does not make mention of impact assessments.

Data processing registers

Article 45 of the Law establishes a national data protection register. The CNDP is responsible for it and is required to make it accessible to the public. The register includes the files that public authorities are responsible for processing; files processed by private persons; references to published laws or regulations establishing public records; the authorisations issued; and data relating to files which are necessary to enable data subjects to exercise their rights to information, access, rectification, deletion and objection.

The CNDP also establishes a list of the types of processing of personal data which are not likely to infringe on the rights and freedoms of data subjects. For these types of processing, the prior declaration to the CNDP only needs to specify the description, characteristics and purpose of the data processing, the categories of data subjects, the recipients and any transborder transfer envisaged.

The CNDP also establishes a list of non-automated processing activities that may be subject to a simplified declaration.

Terms of service icons

The Law does not make mention of terms of service icons.

Additional transparency obligations

There are no further transparency obligations.

Participation

Data subject participation

Articles 5 and 7 of the Law outline the rights of data subjects concerning personal data related to them, which include the following:

- ***Access to personal information:*** data subjects have the right to know about the processing of data concerning them, details about the processing, and to access the data, subject to some exclusions.

- ***Correction, destruction or deletion:*** the data subject has the right to request the correction or deletion of data that is incomplete or incorrect. This right also applies to third parties to whom the data has been communicated. In such cases, the responsible party must undertake the corrections at no cost to the applicant within ten days;

- ***Destruction or deletion of a record:*** A data subject may request a responsible party to destroy or delete personal information about the data subject that the responsible party is no longer authorised to retain, or which was not legally collected.

In the event that a responsible party refuses or does not respond to requests for correction, destruction or deletion of data within the defined period, the data subject may submit a request for correction to the CNDP, which will investigate and have the necessary corrections made as soon as possible, while keeping the data subject updated.

Policy participation

Article 28 of the Law empowers the CNDP to provide its opinion to government and parliament on legal or regulatory propositions or projects relating to the processing of personal data. Similarly, the CNDP is responsible for assessing elements within their purview at the request of public authorities, particularly judicial authorities, assisting the government in defining national priorities and positions during international negotiations in the field of personal data protection, and cooperating with similar bodies controlling the processing of personal data in foreign states.

Enforcement

Supervisory authority

The Law establishes the National Commission for the Control of the Protection of Personal Data ('the CNDP') charged with implementing and ensuring respect for the provisions of the Law. The CNDP is tasked with informing the public and data subjects of their rights and obligations.

It has investigative and inquiry powers, and the power to order the erasure or destruction of data or to temporarily or permanently halt the processing of personal data.

Its responsibilities include:

- ***Receiving complaints from any data subject*** who considers that they have been harmed by the processing of personal data, investigate them and follow up by ordering the publication of corrections and/or referring cases to the public prosecutor for the purposes of prosecution;

- ***Providing its opinion*** to government and parliament on legal or regulatory propositions or projects relating to the processing of personal data or on registration in the national register;

- ***Receiving notifications and declarations*** relating to the local representatives of foreign-based responsible parties, prior declarations of processing, notification of controllers as detailed in Article 19, and providing receipts where necessary;

- ***Providing authorisations*** for data retention, supplementary delays to respond to data subject requests, and processing of sensitive data;

- ***Ensuring corrections*** are made when responsible parties refuse to proceed according to the demands of data subjects;

- ***Determining the list*** of categories of data processing that require only a simplified declaration, or that are exempt from declarations by virtue of relating to public registers, per Article 18;

- ***Establishing a list of countries*** wherein legislation regarding data protection is adequate;

- ***Authorising the transfer of data*** to foreign countries;

- ***Maintaining the national data protection register*** as provided for in Article 45;

- ***Granting exemptions*** or withdrawing authorisations or declaration receipts;

- ***Assessing elements within their purview*** at the request of public authorities, in particular judicial authorities, during disputes;

- ***Assisting the government*** in the preparation and definition of the Moroccan position during international negotiations in the field of personal data protection;

- ***Cooperating with similar bodies*** controlling the processing of personal data in foreign states.

Criminal offences

Chapter VII lays out the sanctions for violations of the Law. These range from obstructing the work of the CNDP, to all forms of illegal processing of data such as unauthorised processing of sensitive data, retaining data beyond the authorised period, or violating the conditions for consent.

When the perpetrator of an offence is a juristic person, the fine is doubled, without prejudice to the penalties which may be applied to its directors if responsible. In addition, the juristic person may be punished with partial confiscation of their property or closure of their establishment(s).

For repeat offences, the penalties are doubled. A repeat offence constitutes committing an offence of the same nature within a year.

Civil remedies

The Law does not make mention of civil remedies, or the possibility of a class action.

Administrative fines

The Law provides for administrative fines for data processing without valid declaration receipts or authorisations, and, obstructing the work of the CNDP.

Offence	Category	Consequence
Processing data without a valid declaration receipt or authorisation	Administrative	10,000 to 100,000 DH
Refusing a data subject's right to access, correct or object	Administrative	20,000 to 200,000 DH
Collecting personal data in a fraudulent, unfair or illicit manner, or processing data for a different purpose to that declared or authorised or in a way incompatible with those purposes	Criminal	Imprisonment of 3 months to 1 year and/or a fine of 20,000 to 200,000 DH
Data retention beyond the duration allowed by law or by the receipt of declaration	Criminal	Imprisonment of 3 months to 1 year and/or a fine of 20,000 to 200,000 DH
Processing in violation of the requirements for consent	Criminal	Imprisonment of 3 months to 1 year and/or a fine of 20,000 to 200,000 DH
Processing of sensitive personal data without consent	Criminal	Imprisonment of 3 months to 1 year and/or a fine of 50,000 to 300,000 DH
Data processing without taking the necessary security precautions as laid out in Articles 23 and 24 of the Law	Criminal	Imprisonment of 3 months to 1 year and/or a fine of 20,000 to 200,000 DH
Processing of personal data of a natural person against that person's wishes, if their opposition is legitimate or the processing relates to direct marketing per Articles 9 or 10	Criminal	Imprisonment of 3 months to 1 year and/or a fine of 20,000 to 200,000 DH
Illegal transfer of data to a foreign country	Criminal	Imprisonment of 3 months to 1 year and/or a fine of 20,000 to 200,000 DH
Causing or facilitating the abusive or fraudulent usage of processed data, or receiving or communicating data to an unauthorised third party, either through negligence or intent	Criminal	Imprisonment of 3 months to 1 year and/or a fine of 20,000 to 200,000 DH. The court may also order the seizure of the material used to commit the offense as well as the erasure of all or part of the personal data
Hindering the work of the CNDP, or refusing to send documents or information	Criminal	Imprisonment of 3 to months and/or a fine of 10,000 to 50,000 DH
Refusing to implement the decisions of the CNDP	Criminal	Imprisonment of 3 months to 1 year and/or a fine of 10,000 to 100,000 DH

NIGERIA

As at 17 September 2020

COUNTRY OVERVIEW			Ref
Is there a comprehensive data protection law?	☐	The Draft Data Protection Bill, 2020 has been published but is not yet in force.	Bill link
Does the law establish a supervisory authority?	☒	Yes, the Bill establishes the Data Protection Commission.	S7(1)
Does the law define the term "personal information"?	☒	The term "personal data" is defined in the Bill and it specifies the type of information the Bill applies to.	S66 ; S4
Does the law prohibit the processing of certain types of personal information?	☒	As a general principle, the Bill prohibits the processing of Sensitive Personal Data.	S26
Does the law prescribe its scope of application?	☒	Yes, the Bill applies to natural and legal persons, and Government entities.	S2(3)
Does the law apply extra-territorially?	☒	Yes.	S2(1)(C)(iv)
Does the law set out conditions for the lawful processing of personal information?	☒	The Bill provides the principles and basis for the lawful processing of personal data.	S3
Does the law stipulate the requirements for valid consent?	☒	In order for consent to be valid, it must be a freely given, specific, informed and unambiguous indication of the data subject's wishes.	S66
Does the law require opt-in consent?	☐	The law is not clear. It notes that the data subject's wishes may be indicated by a statement or by clear affirmative action.	S66
Does the law require notification in the event of a data breach?	☒	In the event of a data breach of personal information, the Data Subject has a right to be notified.	S17
Can personal information be transferred to a third party in a foreign country?	☐	As a general principle, the Bill prohibits the transfer of personal information to a third party in a foreign country. This is subject to certain exceptions.	S43
Does the law require a data protection impact assessment to be conducted?	☒	No.	N/A
Does the law require data processing registers?	☒	No.	N/A

Does the law prescribe the use of terms of service icons or an equivalent measure to inform consent of data use?	☐	No.	N/A
Does the law prescribe penalties for non-compliance?	☒	The Bill provides for criminal, civil and administrative penalties for non-compliance.	S44 - 50

LEGAL ANALYSIS

Legal framework

The Draft Data Protection Bill, 2020 (the Bill) was published on 20 August 2020. At the time of review it was open for comment and in the process of public consultation.

The object of the Bill is to establish a regulatory framework for the protection of personal data. The explanatory memorandum simply notes that the Bill establishes the Data Protection Commission which is responsible for the protection of personal data, the rights of data subjects and the regulation of personal information. One of the objects of the Bill, outlined in section 1(c) is the promotion of a practice that ensures privacy without unduly undermining the legitimate interests of commercial organisations and government security agencies.

Key definitions

The Bill applies to the collection, storage, processing and use of personal data. It provides two definitions for data processing, one of which relates to data processing in the context of non-automated processing.

- The term "***data processing***" is defined to mean: any operation or set of operations performed on personal data such as –
  (a) Collection, recording, organisation, structuring, storage or preservation;
  (b) Adaptation or alteration;
  (c) Access, retrieval or consultation;
  (d) Transmission, disclosure, sharing or making available; or
  (e) Restriction, erasure, or destruction of, or the carrying out of logical or arithmetical operations.

- "Data processing" where automated processing is not used, is defined to mean "an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria."

In terms of the relevant role-players, the key definitions include the following:

- The term "***data subject***" means the identifiable living natural person to whom the personal information relates. It accordingly excludes juristic or legal persons.

- The term **"identifiable data subject or identifiable natural person**" means a natural person who can be identified directly or indirectly, by reference to an identifier such as a name, identification number, online identifier, and includes singling-out a natural person.

- The term "***data controller***" means the natural or legal person which alone or jointly with others has decision-making power over the purposes and means of data processing. It specifically includes public authorities, services, Commissions and any other body. Section 30(2) explicitly notes that a data controller includes a Ministry, department, agency and other public institutions of government.

- The term "***data processor***" means the natural or legal person, public authority, service commission or other body, which alone or jointly, processes personal data on behalf of the data controller.

The following definitions are also of relevance:

- The term "***personal data***" is defined to mean any information relating to an identified or identifiable natural person. Section 4 specifies the categories of data which the Bill applies to, and is outlined in detail below.

Scope of application

Requirements for the scope of application

The Bill applies to "the collection, storage, processing and use of personal data relating to persons residing in Nigeria and persons of Nigerian nationality, by automated and non-automated means, irrespective [of] residence."

The scope of application further notes its application to private and public sectors in Nigeria and to data controllers and processors in the following circumstances:

- The data controllers and processors are established in Nigeria, they process personal data within Nigeria and the data they process concerns data subjects in Nigeria;
- The data subject resides within or outside Nigeria;
- The data controller is not established in Nigeria, but uses equipment or a data processor in Nigeria to process the personal data of data subjects who reside within or outside Nigeria; or
- Processing is carried out in respect of information relating to data subjects who reside within or outside Nigeria and personal data which originates partly or wholly from Nigeria.

This raises the following considerations:

- ***Processing of personal information:*** there must be processing of personal data.

- ***Automated or non-automated means:*** it is irrelevant whether the data controller makes use of automated or non-automated means. Automated means is not defined in the Bill,and there are no additional requirements for non-automated means such as its inclusion in a filing system.

The Bill includes a useful section which lists the individuals and entities which must comply with the Bill, it includes:

- A data subject who is a Nigerian citizen;
- A data subject who is ordinarily resident in Nigeria;
- A body incorporated under the laws of Nigeria;
- An unincorporated joint venture or association operating partly or completely in Nigeria;
- Any person who maintains an office, branch or agency which carries out business activities in Nigeria;
- Foreign entities targeting persons resident in Nigeria.

This list does not explicitly include public bodies or authorities despite their inclusion in the definition of ***data controller.*** It is unclear what 'targeting persons resident in Nigeria' refers to as 'targeting' is not defined or referred to again in the Bill.

Section 30(2) explicitly notes that a data controller includes a Ministry, Department, Agency and other public institutions of government.

What information does the law apply to?

Section 4 lists the categories of data which the Bill applies to, it includes:

"(a) personal and biometric data revealing a data subject's identity, racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation or trade union membership;
(b) personal banking and accounting records;
(c) personal data revealing a data subject's flight reservation or itinerary;
(d) Student's academic transcripts records;
(e) personal medical and health records;
(f) telephone calls, call data records, messages, websites, and other information stored on any electronic device;
(g) personal subscription data which reveals data subject behaviour; and
(h) such other categories of data usually processed by service providers and commercial entities as may be determined by the guidelines of the Commission to be protected under this Act"

The definition of a data subject appears to exclude data concerning a juristic person. However, the wording of this section may be interpreted to include data relating to juristic persons; for example, accounting records and information stored on electronic devices is not explicitly referred to as relating to a data subject.

Compliance by data controllers

The Bill applies to data controllers which are defined to include natural and legal persons, public authorities and any body which determines the purposes and means for processing personal data.

The Bill applies to foreign entities if they use equipment or a data processor which operates in Nigeria, and they process the personal data concerning data subjects who reside within or outside Nigeria. Section 2(1)(c)(iv) notes that the Bill applies to data controllers which process information concerning data subjects which reside within or outside Nigeria and personal data which originates partly or wholly from Nigeria, this broadens the scope of application significantly.

Compliance by data processors

The Bill also applies to data processors that process personal data for a data controller. The Bill provides for vicarious liability and the data controller is accordingly liable for the data processing carried out on its behalf by a data processor.

Section 31(1) prescribes that only data processors which provide appropriate technical and organisational measures may be used by a data controller. Any processing done by a data processor must be provided for in a contract which includes details concerning the nature of the processing and any penalties for breach.

Section 32 outlines the duties of a data processor, some of which include a prohibition on engaging a further data processor without authorisation from the data controller; a duty to inform the data controller of any legal requirements which may create risks to a data subjects rights and to only process data on written instructions form the data processor.

If a data processor engages a third party to process data on its behalf, the same contractual requirements apply and the data processor is liable to the data controller for ensuring the third party's obligations.

Exclusions

The Bill provides for certain exclusions from its scope of application. The exclusions include the following:

- ***Personal or household activity:*** processing of personal data in the course of a purely personal or household activity. "Household activity" is defined as activities which are closely linked to the private life of an individual, which don't impede on the personal sphere of others and have no commercial intent.

Section 35(1) states that the privacy of personal data is exempt from the requirements of the Bill for the following purposes:

- ***Public interest:*** the exception in section 35(1) is titled public interest and simply includes the following list – public order; public safety; public morality; national security; public interest; the prevention or detection of crime; apprehension or prosecution of an offender; the assessment or collection of a tax or similar duty; or publication of a literary or artistic material. None of these terms are defined in the Bill. The only additional information provided by the Bill is included in section 35(4) which notes that when determining whether a publication is in the public interest, regard may be had to a code of conduct.

- ***Protection of the public:*** this exemption notes that processing does not have to comply with the bill when it is done to protect members of the public against loss concerning professional services such as banking and investment; dishonesty or malpractice; misconduct of a non-profit organisation or to secure the health or welfare of people at work.

- ***Research:*** if personal data is only processed for research purposes, it is exempt from the Bill if it is processed in compliance with the relevant provisions and the results are not made available in a form which identifies a data subject. Further processing used for research will be considered compatible with the purpose and may be retained indefinitely.

- ***Court order:*** the provisions of non-disclosure are not applicable if such disclosure is required by law or by court order.

- ***Service or education:*** the processing of personal data is exempt from the principles of the Bill if it consists of a confidential reference provided by the data subject in the course of education or employment; the appointment to an office or for the provision of any service.

- ***Combat effectiveness:*** this exemption notes that personal data is exempt from the subject information provisions if their application is likely to prejudice the combat effectiveness of the Nigerian Armed Forces. The Bill does not specify what the subject information provisions include, nor are they referred to elsewhere in the Bill.

- ***Employment:*** section 35(10) notes that the Commission may make regulations and guidelines which prescribe exemptions concerning government employment or appointment to public office.

Rights of data subjects

The Bill sets out the following rights of data subjects, which include the following:

- ***Access:*** the right to establish whether their personal data has been processed, including information concerning its origin and the reason for its processing. If requested a copy of the data must be provided within one month.

- ***Automated decision-making:*** the right not to be subject to a decision which is based solely on automated processing of data which significantly affects her without her views being considered. This does not apply when the decision is authorised by law and provides for appropriate measures to safeguard the rights and freedoms of the data subject.

- ***Rectification, erasure and restitution***: the right to rectification, blockage or erasure of inaccurate, false or unlawfully processed personal data.

- ***Judicial remedy:*** the data subject has a right to judicial remedy where the provisions of the Bill have been violated.

- ***Objection:*** the right to object to the processing of their personal information, including profiling. They may further object to processing for the purposes of direct marketing.

- ***Suspension:*** this right notes that a data controller shall no longer process personal data unless the data controller demonstrates legitimate grounds or interests for processing which override the rights and interests of the data subject.

- ***Prevention:*** the data subject may request a data controller to cease or not begin processing data which is not lawful and is likely to cause unwarranted damage or distress. This may be done at any time. The data controller must inform the data subject, within one month, that it has or intends to comply or provide the reasons for non-compliance.

- ***Data Portability:*** the right to receive their personal data in a commonly used, machine-readable format and to submit it to another data controller without hindrance. This right does not apply to data which is necessary for the performance of a task in the public interest or an exercise of official authority.

Conditions for the lawful processing of personal information

The Bill prescribes eight basic principles for the lawful processing of personal data. Processing must be carried out based on these principles, which include:

- ***Purpose:*** personal data must be processed for specific, explicit and legitimate purposes;

- ***Processing limitation***: personal data must be processed in a lawful, fair and transparent way;

- ***Further processing limitation:*** any further processing must be compatible with the purpose for which it was initially collected;

- ***Scientific, historical, scientific:*** this principle notes that personal data must be processed for archiving, scientific, historical research and statistical purposes in accordance with any relevant laws;

- ***Purpose specification:*** this principle requires that the processing be adequate, relevant and limited to what is necessary for the purpose;

- ***Data quality:*** requires that the personal data be accurate and regularly kept up to date;

- ***Security Safeguards:*** personal data must be processed in a manner which ensures appropriate security of the personal data, including protection against unlawful access, loss or damage;

- ***Retention:*** the data must be kept in a form which allows for identification only for as long as necessary. It must be deleted once its purpose has been achieved or kept in a form which prevents any direct or indirect identification.

The Bill further prescribes, in section 4(2), the legal basis for processing personal data. This section must be read with section 2(1)(a)(i) which requires that personal data be processed on the basis of an individual's consent or another specified lawful basis. These additional specified lawful bases include:

- The performance or commencement of a contract which the data subject is a party to;
- Compliance with a legal obligation which applies to the data subject;
- The protection of the data subject or another person's vital interests, where vital interest refers to those relating to life and death issues;

- The performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
- The purpose of prevailing legitimate interests of the data controller or third party, unless they are overridden by the interests, rights or freedoms of the data subject.

Section 51(1) prohibits a person who provides goods, facilities or services to the public from requiring that someone produce or supply a record as a condition for the provision of such goods or services. A record is not defined in the Bill.

Restrictions on the processing of personal information

Sensitive data

The Bill prohibits the processing of sensitive data, subject to certain exceptions. Sensitive data includes information relating to a child under parental or guardian control and a data subject's religious or philosophical beliefs; race or ethnic origin; political opinions; health; sex life or behaviour.

The prohibition on the processing of sensitive data does not apply if the processing is necessary as provided for by the Bill or the data subject consents. For the purposes of processing a child's data, the consent of the parent or guardian is required.

The bill provides the circumstances which would make the processing of sensitive data necessary, these include:

- ***Exercise of a right***: processing the data is necessary for the exercise or performance of a right imposed by law on an employer;

- ***Protection of a vital interest***: processing is necessary for the protection of the vital interests of the data subject where its impossible to obtain consent from the data subject or its impossible to expect the data controller to obtain it. The wording of this provision is unclear but it appears necessary for an affidavit to be drafted by the data controller to this effect.

- ***Legitimate activities***: processing is necessary for the protection of the legitimate activities of a body or association which is established for non-profit purposes or exists for political, philosophical, religious or trade union purposes. The processing must relate to their members and must not be disclosed to a third party without the data subjects consent.

- ***Required***: sensitive data may be processed when it is required for legal proceedings; for the establishment or defence of legal rights; in the course of the administration of justice or for medical purposes by a health professional bound by a duty of confidentiality.

- ***Elimination of discrimination***: sensitive data concerning race or ethnic origin may be processed if it is necessary for the elimination of discriminatory processes and carried out with appropriate safeguards.

- ***Religious beliefs***: sensitive data concerning religious or philosophical beliefs may be processed by a spiritual or religious organisation if the processing concerns the data of its members and its necessary for its purpose.

Direct marketing

The Bill prohibits the provision, use or procurement of personal data for the purposes of direct marketing without the prior written consent of the data subject. Direct marketing is defined to include the communication, by whatever means, of any advertising or marketing material which is directed at a particular data subject.

The Bill provides data subjects with the right to object to processing for the purposes of direct marketing. The data subject may do so at any time and is then entitled to have the data unconditionally erased, removed or supressed. Upon receipt of a complaint that the data controller has not complied, the Commission may order compliance.

Automated decision-making

The Bill provides data subjects with the right not to be subject to a decision which is based solely on automated processing. Section 28(1) requires that data subjects must not be subjected to a decision in violation of this right.

In the event that such a decision has been taken, the data controller must notify the data subject as soon as reasonably practical and the data subject is entitled to request the data controller to reconsider the decision within 21 days. The data controller must inform the data subject, within 30 days, of the steps which it intends to take to comply. If the data controller fails to comply, the data subject may lodge a complaint with the Commission and the Commission must order compliance.

Automated decision making is not prohibited in the following circumstances:
- In considering whether to enter into a contract with the data subject;
- In the performance of such a contract;
- For a purpose authorised by an enactment; or
- In other circumstances prescribed by the Commission.

Transborder data transfers

The Bill provides that the trans-border transfer of personal data is only permitted if an adequate level of protection exists or because of the applicability of certain exceptions.

- ***Adequate level of protection****:* An adequate level of protection must be secured in the recipient country which includes:

    - The applicability of data protection laws, treaties or agreements;
    - Approved safeguards which have been provided by legally binding and enforceable instruments adopted by data controllers and processors involved in the transfer;
    - Section 43(2)(a) simply lists "adequacy, accountability, authorization and reciprocity in the recipient State". None of these terms are defined nor does the Bill specify what is required they require.

    If data is transferred under this justification, then all relevant information concerning the transfer must be provided to the Commission.

- ***Consent:*** the data subject has provided consent which is explicit, specific and free. If requested to do so, then all information concerning a transfer made under this justification must be submitted to the Commission.

- ***Interest of the data subject:*** the specific interests of the data subject require the transfer in a particular case. The Bill does not specify any considerations for such a determination. If requested to do so, then all information concerning a transfer made under this justification must be submitted to the Commission.

- ***Legitimate interests:*** data may be transferred if "prevailing legitimate interests, in particular important public interests, are provided for by law". The Bill does not define public interest, nor does it specify any considerations for such a determination. If requested to do so, then all information concerning a transfer made under this justification must be submitted to the Commission.

The Commission is empowered to request a demonstration of the effectiveness of safeguards or the existence of prevailing legitimate interests. Transfers may be prohibited, suspended or subjected to specified conditions. The Commission must ensure that any onward transfer, following the initial transfer, shall meet the minimum requirements for transfer of personal data. It is unclear what constitutes such minimum requirements.

Requirements for consent

Consent is one of the justifications for the lawful processing of personal information. Section 5(1) places the burden of proof on the data controller and notes that consent must represent the free expression of an intentional choice which can either be given by a statement or by a clear affirmative action. Such consent may be withdrawn at any time and doing so does not affect the lawfulness of previous processing.

The legislative framework does not expressly prohibit discrimination for declining consent.

Transparency

One of the objects of the Bill is to ensure that personal data is processed in a transparent manner. This is detailed in section 6(1) which provides data subjects with a right to be informed about the processing of their data. It reiterates the requirement that processing must be conducted fairly and transparently.

The data controller is obligated to inform the data subject of the following details:

- its own official identity and contact details;
- the contact details of the data controller;
- the basis and purpose of the processing;
- the categories of personal data processed;
- The recipients of the personal data;
- Any intended transfer to a third party or foreign country and the safeguards in place;
- The retention period;
- The existence of automated decision making and the right to object and challenge it;
- The existence of profiling and its consequences;
- The right to withdraw consent if the processing is based on consent.

The Bill requires that the above information be provided in an appropriate format, using plain language and where the personal data is not collected directly from the data subject, the data subject must be informed no later than one month or on first communication. This does not apply where the processing is expressly prescribed by the Bill or any other legislation.

Notification of a data breach

The Bill does not deal extensively with the breach notification; it is simply noted as a right and includes some detail on the content requirements of the notification.

Data subjects have a right to be notified of a data breach affecting them within 48 hours after notification to the Commission. The Bill does not stipulate the time required for notification to the

Commission. The notification must include a description of the nature of the breach, the contact information of the data protection officer, details of the probable consequence and describe the measures taken to address it.

Impact assessments

The Bill requires that before processing, a data controller must examine the likely impact of the processing on the rights and freedoms of data subjects. This is prescribed under section 30 which deals with the duties of data controllers and processors. It does not specifically refer to this examination as an impact assessment and does not prescribe conditions for publication or its submission to the Commission.

Data processing registers

The Bill does not require a data processing register.

Terms of service icons

The Bill does not require the use of terms of service icons.

Additional transparency obligations

In addition to the above, the following measures may also serve to enhance transparency:

- ***Audit report:*** every data controller and processor must submit a data protection audit report to the Commission. The Commission will publish an annual report containing a list of the organisations which submitted their audit reports. It appears that the audit reports will not be made publicly available and the Bill does not specify what must be included in such a report.

- ***Annual reports:*** within six months of each financial year, the Commission is required to submit a report to the president which details its activities of the preceding year, including its audited accounts and auditor's report.

- ***Record of activities:*** data processors must maintain a record of processing activities. The Bill does not stipulate whether such record must be submitted to the Commission or made publicly available.

Participation

Data subject participation

The Bill does not expressly include data subject participation as a principle for the lawful processing of personal data, instead it refers to the right of access which includes the following:

- ***Access to personal data:*** a data subject has the right to request a data controller to confirm whether or not it processes personal data about the data subject; and to request a copy of the personal data as well as all available information such as the origin of the data.

- ***Rectification, erasure and restitution:*** a data subject has the right to rectification, blockage or erasure of inaccurate, false or unlawfully processed personal data.

- ***Objection:*** a data subject has the right to object to the processing of their personal information, including profiling. They may further object to processing for the purposes of direct marketing.

- ***Data Portability:*** a data subject has the right to receive their personal data in a commonly used, machine-readable format and to submit it to another data controller without hindrance. This right does not apply to data which is necessary for the performance of a task in the public interest or an exercise of official authority.

- ***Request assessment:*** a person who is affected by the processing of any personal data may request the Commission to make an assessment of whether such processing complies with the Bill.

Policy participation

The Commission is empowered to review guidelines and regulations made under the Bill. It may review, process, modify, vary or repeal them if they are no longer relevant; no longer necessary in the national interest; not necessary to achieve the object of the Bill; or for any other reason the Commission considers necessary to give effect to the Bill.

Enforcement

Supervisory authority

The Bill establishes the Data Protection Commission (the Commission). In this regard, the Commission is a body corporate with perpetual succession which is capable of suing and being sued and acquiring property. The Bill requires that the Commission act with complete independence and impartiality when performing its functions.

The Commission must provide the process to obtain, use or disclose personal information; ensure compliance with the Bill; assist the facilitation of the free flow of personal data; promote awareness of the rights of data subjects and consult on policy and legislative measures which impact personal data.

One of the functions of the Commission is to act as the supervisory authority and exercise regulatory powers, in this regard it must:

- Approve risk management processes for data controllers and processors to ensure compliance;
- Issue directives in the event that operations are likely to infringe with the Bill;
- Receive and process complaints from data subjects whose rights have been infringed;
- Order the rectification, completion or deletion of personal data and impose temporary or permanent limitations on the processing which may include a ban;
- Impose administrative fines or sanctions where data controllers and processors infringe a provision of the Bill.

The Commission is empowered to implement and monitor compliance with the Bill; investigate any complaint under the Bill and determine it in a manner which it considers fair; impose fines and penalties to enforce compliance and seek redress. It may apply to a court for a warrant necessary for the performance of its functions, and may execute its duties with the assistance of law enforcement agencies.

It is important to note that although the Bill recognises liability for offences committed by members of the Commission, it prescribes that such claims must be instituted within three months after the ceasing of such act. It further requires that no suit may commence before the expiry of one month after notifying the Commission of the intention to do so.

Enforcement Notice

If a data controller or processor has contravened any of the data protection principles prescribed in the Bill, the Commission is obligated to serve them with an enforcement notice. Such a notice may also be served if the Commission reasonably believes that a contravention is likely to occur.

Such notice may request the data controller to take certain steps or refrain from processing data as specified. It may require that the data controller rectify, block, delete or destroy personal data.

Importantly, such an enforcement notice may be cancelled or varied by the Commission on its own initiative or upon application of the recipient of such a notice. This provision does not require notice be provided to any affected data subjects nor does it specify the considerations which must be taken into account when doing so. It is accordingly unclear what accountability mechanisms are provided for in the Bill.

Failure to comply with a notice is an offence and liability includes the imposition of a fine, the amount of which is determined by the Commission.

Section 42(1) provides that the Commission may authorise an officer to perform its enforcement functions. Such an officer may enter to inspect and search any premises, systems or equipment, under warrant issued by a court. They may further seize, seal or remove anything which contains evidence of the commission of an offence under the Bill. The warrant may also authorise them to use any device to search any data and to use any technology to decode or decrypt any coded or encrypted data. The Bill does not define 'officer' and it is accordingly unclear who would constitute such a designation.

Such a warrant may be applied for by an officer of the Commission, ex-parte to a Judge in Chambers. The Judge must be satisfied that there are grounds to believe that an activity which contravenes the Bill is taking place or is likely to take place. The Judge must be further satisfied that the warrant is sought to prevent the commission of an offence; it is for the purpose of investigating cybercrime or computer related offences; there are grounds to believe the person or equipment is relevant to the commission of the offence; or the object or subject is preparing to commit an offence under the Bill. This section appears to widen the scope for the issuance of a warrant beyond the prevention of a contravention of the Bill; the Bill does not relate to 'cybercrimes' or 'computer-related offences', nor are these detailed or defined anywhere in the Bill.

Data Protection Officer

The Bill prescribes that a data controller must appoint a data protection officer who will be responsible for ensuring compliance with the Bill. It notes that such appointment is subject to regulations which will be drafted by the Commission.

Criminal offences

Certain criminal offences are created under the Bill. Some of these include the selling of personal data which was knowingly or recklessly obtained or disclosed to a third party without the consent of the data controller and the unlawful disclosure of personal data by a member of the Commission.

Certain contraventions carry a penalty of a fine of ten million Naira and/or imprisonment of up to 5 years.

In addition, the Bill empowers a court to order that a convicted person forfeit any proceeds of the offence to the Government of the Federal Republic of Nigeria. They are also empowered to order the forfeiture of any device or software that was used to commit or facilitate the commission of the offence. This includes assets in a foreign country.

Civil remedies

Section 29(1) provides that a data subject may approach a court to institute a claim for damages for non-compliance with the Bill. This section notes that such a claim may be instituted against either the data controller or the data processor. Section 31(1) of the Bill, however; provides for vicarious liability and states that the data controller is liable for the data processing carried out on its behalf by a data processor.

The fault requirement is not specified but it provides that proof of reasonable care constitutes a valid defence.

Section 50(1) empowers a court to order a data controller, processor or person convicted under the Bill, to compensate or make restitution to the victim of the offence. Such an order may be enforced by the victim or the Commission in the same way as a judgment in a civil action.

The Bill does not specifically provide for the institution of a class action.

Administrative fines

The Bill provides for the provision of an administrative fine. Section 41(1) notes that failure to comply with an enforcement notice is an offence and liability includes the imposition of a fine. The amount of the fine is determined by the Commission, but no considerations are outlined for such a determination.

Offence	Category	Consequence
Knowingly or recklessly obtaining or disclosing personal data to a third party without the consent of the data controller[1]	Criminal	A fine of not less than five million Naira or imprisonment for a term not less than 1 year, or both
Retaining personal data without the consent of the data controller	Criminal	A fine of not less than five million Naira or imprisonment for a term not less than 1 year, or both
Selling personal data which was knowingly or recklessly obtained or disclosed to a third party without the consent of the data controller	Criminal	A fine of not less than one million Naira or imprisonment for a term not less than 5 years, or both
Advertising data in a manner which indicates it was obtained knowingly or recklessly without the consent of the data controller	Criminal	A fine of not less than five hundred thousand Naira per record or imprisonment for a term not less than 5 years, or both
Failure by a data controller or processor to implement appropriate data protection safeguards, policies and standards	Criminal	A fine of not less than ten million Naira for every year in default or imprisonment for a term not less than 1 year, or both
Obstructing the execution of a warrant	Criminal	A fine of not less than five million Naira or imprisonment for a term not less than 6 months, or both
Failure to assist with the execution of a warrant	Criminal	A fine of not less than five million Naira or imprisonment for a term not less than 6 months, or both
In compliance with a notice, a person provides a statement knowing it to be false in a material respect	Criminal	A fine of not less than five million Naira or imprisonment for a term not less than 1 year, or both
In compliance with a notice, a person recklessly provides a statement which is false in a material respect	Criminal	A fine of not less than five million Naira or imprisonment for a term not less than 1 year, or both
Attempts to commit any offence under this Bill	Criminal	Liable to the punishment provided for the principal offence under this Bill
Aids, abets, conspires, counsels or procures another person to commit any offence under this Bill	Criminal	Liable to the punishment provided for the principal offence under this Bill

[1] Section 44(1) explicitly notes the consent of a data controller, it is unclear if it was erroneously included instead of requiring the consent of the data subject or if this section only applies to data processors.

A staff member of the Commission knowingly or recklessly discloses information which was obtained during the course of the function of the Commission, relates to an identifiable data subject and is not publicly available	Criminal	A fine of not less than ten million Naira or imprisonment for a term not less than 2 years, or both
A data subject suffers damage through the contravention of the Bill	Civil	Damages
Failure to comply with an enforcement notice	Administrative	Fine determined by the Commission.

SENEGAL

As at 18 September 2020

COUNTRY OVERVIEW			Ref
Is there a comprehensive data protection law?	☒	Law No. 2008-12 of 25 January 2008 (LDCP).	Law link
Does the law establish a supervisory authority?	☒	The Law establishes the Commission for Data Protection (CDP).	Article 5
Does the law define the term "personal information"?	☒	The term "personal information" is defined in section 3 of the law.	Article 4(6)
Does the law prohibit the processing of certain types of personal information?	☒	The law prohibits the processing of certain types of personal data, referred to as "sensitive personal information", subject to certain exceptions.	Article 40
Does the law prescribe its scope of application?	☒	The law applies to both public and private bodies, as well as natural and juristic persons. Foreign entities, which are not domiciled in Senegal, must comply if they process data using methods of processing in Senegal or do more than simply forward personal information through Senegal.	Article 2
Does the law apply extra-territorially?	☐	No.	Article 2
Does the law set out conditions for the lawful processing of personal information?	☒	The law contains at least six conditions for the lawful processing of personal data.	Chapters III and V
Does the law stipulate the requirements for valid consent?	☒	The law stipulates that in order for consent to be valid, it must be an express, unequivocal, free, specific and informed manifestation of will.	Article 4
Does the law require notification in the event of a data breach?	☐	No.	N/A
Can personal information be transferred to a third party in a foreign country?	☒	Data may be transferred if sufficient protections are in place.	Articles 49-51
Does the law require a data protection impact assessment to be conducted?	☐	No.	N/A
Does the law require data processing registers?	☐	No.	N/A

Does the law prescribe the use of terms of service icons?	☐	No.	N/A
Does the law prescribe penalties for non-compliance?	☒	The law provides for one penalty for failure to comply with CDP notices; other violations are provided for in the Penal Code and the Cybercrime Law.	Article 30 and Chapter VI

LEGAL ANALYSIS

Legal framework

Law No. 2008-12 of 25 January 2008 (the LDCP) concerning the Protection of Personal Data was enacted to curb privacy violations caused by the collection, processing, transmission, storage and use of personal data. The law regulates the processing of personal data to ensure respect for the rights, fundamental freedoms and dignity of natural persons.

The state, public entities, local authorities and private legal persons managing a public service carrying out data processing had two years from the date the LDCP came into operation to become compliant, while all other entities had one year.

In addition to the LDCP, the legal framework further comprises *Decree No 2008-721 of 30 June 2008 Concerning the Application of Law no. 2008-12 of 25 January 2008 on the Protection of Personal Data Law* (the Decree). The Decree outlines the functions of the Commission for the Protection of Personal Data (CDP), the rights conferred on data subjects, the obligations of responsible parties, and details the implementation of sanctions for violations of the law.

The LDCP also states that the automated processing of identifiable information carried out on behalf of the state, a public entity, local authority or juristic person bound by private law managing a public service is decided by regulatory act after reasoned opinion by the CDP.

Furthermore, Article 78 of the LDCP provides for a specific regulatory provision to deal with the application of the law to the digitised Senegalese national identity card, due to the specific nature of the matter. Law No. 2016-09 of March 14, 2016 and Decree No. 2016-1536 fulfils this requirement by establishing an ECOWAS biometric ID card.

Key definitions

The definitions are set out in Section 3 of the LDCP. In terms of the relevant role players, the key definitions include the following:

- The term ***"data subject"*** is defined to mean any natural person who is subject to processing of personal data.

- The term ***"responsible party"*** is defined to mean any natural or juristic person, either public or private, or any other entity or association who, either alone or jointly with others, takes the decision to collect and process personal data and determines the purposes of such.

- The term ***"sub-contractor"*** is defined to mean any natural or juristic person, either public or private, or any other entity or association that processes personal data on behalf of the responsible party.

- The term ***"recipient"*** is defined to mean any person authorised to receive communications of data other than the data subject, the responsible party, the sub-contractor or the persons who, by reason of their functions, are responsible for processing data.

- The term ***"third party"*** is defined to mean any natural or juristic person, either public or private, or any other entity or association other than the data subject, the responsible party, the sub-contractor and the people who, placed under direct authority of the responsible party or sub-contractor, are authorised to process the data.

The following definitions are also of relevance:

- The term ***"personal data"*** is defined to mean any information relating to a natural person that is identified or identifiable either directly or indirectly by reference to an identification number or to one or multiple elements that are specific to their physical, physiological, genetic, psychological, cultural, social or economic identity.

- The term ***"sensitive data"*** is defined to mean any personal data relating to religious, philosophical, political or trade union opinions or activities, to one's sexual or racial life, health, social measures, prosecutions, or criminal or administrative sanctions.

- The term ***"processing of personal data"*** is defined to mean any operation or set of operations carried out with or without the aid of automated processes, and applied to data, such as the collection, exploitation, registration, organisation, conservation, adaptation, modification, extraction, protection, copying, consultation, utilisation, communication by transmission, distribution or any other form of making available, reconciling or linking, as well as the locking, encryption, erasure or destruction of personal data.

- The term ***"third party country"*** is defined to mean any state other than Senegal.

- The term ***"linkage of personal data"*** is defined to mean any connection mechanism consisting of the linking of processed data for a specific purpose with other data processed for the same or different purposes, or linked by one or more data controllers.

Scope of application

The LDCP applies to the following:

- ***Any collection, processing, transmission, storage and use*** of personal data by a natural person, by the State, local authorities, or legal persons governed by public or private law;

- ***Any automatic or non-automatic processing*** of data contained or intended to appear in a file;

  Any processing carried out by a responsible party on Senegalese territory, in any place where Senegalese law applies, or who uses means of processing located on Senegalese territory, excluding means which are only used for purposes of transit;

- ***Any processing of data concerning public security, defence, research and prosecution of criminal offenses or State security,*** even related to an important economic or financial interest of the State, subject to some exceptions.

What information does the law apply to?

The LDCP applies to the personal data of natural identified or identifiable persons. It does not restrict its scope to Senegalese citizens; rather it protects the personal data of any data subject within Senegal or whose data is processed using means located in Senegal, other than for transit purposes.

Compliance by responsible parties

Processing of personal data must be subject to a declaration to the CDP, which provides receipts of acknowledgement within one month (renewable once), and which must be received before processing can begin. The declaration must conform to a model established by the CDP and must contain a commitment that the processing meets the requirements of the law. Article 22 of the LDCP prescribes the details which must be provided in the declaration, which includes the identity of the responsible party, the purpose of the processing, the duration of the retention of the data, and the ways data subjects can access the data. Any change in these details must be reported to the CDP, along with any deletion.

The following are exempt from prior declarations:

- ***Register:*** processing for the sole purpose of keeping a register which, by virtue of legislative or regulatory provisions, is intended exclusively for the information of the public and is open to consultation by the public or any person showing a legitimate interest;

- ***Associations or non-profit organisations:*** processing carried out by an association or non-profit organisation of a religious, philosophical, political or trade union nature. In order to be exempt, the data must correspond to the purpose of the association, only concern their members, and must not be communicated to third parties.

The CDP publishes a list of the most common forms of personal data processing which are not likely to threaten privacy or freedoms, and for which the CDP defines norms to simplify or do away with the need for a declaration.

In addition, Chapter 5 places the following obligations on responsible parties:

- ***Confidentiality:*** processing may only be carried out under the authority of responsible parties and on its instruction.

- ***Security:*** the responsible party is required to take precautions to protect the security of the data against distortion, damage, or from unauthorised access. Article 71 provides detailed security obligations that responsible parties must comply with.

- ***Retention:*** personal data must only be retained for a period that is necessary, except for historical, statistical or scientific purposes.

- ***Sustainability:*** the responsible party is required to take all necessary measures to ensure that the personal data processed can be used regardless of the technical means used. In particular, they must ensure that the evolution of technology will not be an obstacle to processing.

Compliance by operators

When processing is implemented on behalf of a responsible party, they are required to choose a sub-contractor which provides sufficient guarantees. It is incumbent on responsible party as well as the sub-contractor to ensure compliance with the security measures defined by article 71. The processing must be governed by a written contract or legal act that binds the sub-contractor to the responsible party and which provides that the sub-contractor only acts on the instruction of the responsible party and is bound by the obligations which apply to the responsible party.

Exclusions

The LDCP provides for certain exclusions from its scope of application, which include the following:

- ***Personal or household activity:*** data processing carried out by a natural person in the exclusive framework of their personal or domestic activities is excluded, provided the data is not intended for systematic communication to third parties or for dissemination;

- ***Temporary copies:*** temporary copies made within the framework of the technical activities of transmission and provision of access to a digital network. This must concern the automatic, intermediate and transient storage of data for the sole purpose of enabling other recipients of the service the best possible access to the information transmitted, is also excluded;

- ***Journalistic, research, literary or artistic purposes:*** the processing of personal data carried out for the purposes of journalism, research or artistic or literary expression is permitted when it is carried out for the sole purpose of literary and artistic expression or the exercise, in a professional capacity, of the activities of journalists or researchers, in compliance with the ethical rules of those professions.

Rights of data subjects

The LDCP sets out the following rights of data subjects:

- ***Notification:*** data subjects have a right to be notified about the details of data collection. This includes the purpose for which data is processed, the recipients of the data, whether responses are obligatory and the consequences of a default response. Notification is not required in all circumstances, some of which include data relating to state security, defence, public security, important economic or financial interests of the state and criminal or judicial processes.

- ***Access:*** any natural person has the right to confirm whether their data is subject to processing, to contest the processing of their data, to access their data, and to receive information about the purpose, recipients, origin of the data, and its transfer to another country. The responsible party may charge a fee for providing a data subject with a copy of their data that is no more than the cost of reproducing it. The right to access may be exercised on behalf of a patient by their doctor or by a family member if the data subject is deceased. For data relating to state security, defence or public security, the right to access is exercised through requests to the CDP.

- ***Objection:*** any natural person has the right to object to the processing of their personal data. This includes the right to be notified before their data is communicated to a third party or used for marketing purposes, except in cases where processing serves a legal obligation.

- ***Correction or deletion:*** any natural person has the right to require a responsible party to correct, complete, update, lock or delete personal data concerning them which is incorrect, incomplete, ambiguous, out of date or illegally collected or processed.

Conditions for the lawful processing of personal information

In addition to the requirement of prior declaration, the law outlines the following conditions for the lawful processing of personal data:

- ***Consent:*** the processing of personal data is only legitimate if the data subject provides their consent, subject to some exceptions;

- ***Processing limitation:*** processing must be done in a lawful, fair, and non-fraudulent manner;

- ***Purpose specification***: processing must be adequate, relevant and not excessive with regard to the purpose for which the data was collected and processed;

- ***Retention limitation:*** data must not be retained for a period longer than that which is necessary for the purpose for which it was collected and processed. After that period, data may only be retained for historical, statistical or research purposes;

- ***Information quality:*** the data collected must be correct and updated, if necessary. Every reasonable measure must be taken to erase or rectify data that is incorrect or incomplete.

- ***Security safeguards:*** personal data must be treated in a confidential manner and protected.

Restrictions on the processing of personal information

Special personal information

It is prohibited to process personal data which concerns racial, ethnic or regional origin, parentage, political opinions, religious or philosophical convictions, trade union membership, sex life, genetic data or health information.

Exceptions to this prohibition include:

- ***Public data:*** personal data has been made public by the data subject;
- ***Consent:*** the data subject has given their consent in writing;
- ***Necessary to protect vital interests:*** it is necessary to protect the vital interests of the data subject or another person and the data subject is physically or legally unable to provide consent;
- ***Necessary for legal claims:*** it is necessary for the establishment, exercise or defence of legal claims. However, genetic data can only be processed to verify the existence of a genetic link in the context of the administration of evidence in court, for the identification of a person, or for the prevention or punishment of an offence;
- ***Legal proceedings***: legal proceedings or a criminal investigation have been initiated;
- ***Public interest:*** it is necessary for reasons of public interest, in particular for historical, statistical or scientific purposes;
- ***Contract***: it is required for the performance of a contract to which the data subject is party or for the execution of pre-contractual measures taken at their request;
- ***Legal obligation:*** it is necessary for compliance with a legal obligation or regulations to which the responsible party is subject;
- ***Public authority:*** it is required for the performance of a task of public interest, is carried out by a public authority, or is assigned by a public authority to the responsible party or to a third party to whom the data is communicated;
- ***Activities of a specific organisation:*** it is carried out within the framework of the legitimate activities of a foundation, association or any other non-profit organisation and for political, philosophical, religious, mutualist or trade union purposes. However, the processing must only relate to its members or persons having regular contact with it, be required for its purpose and the data must not be communicated to third parties without consent.

Processing of some kinds of sensitive personal data is allowed but requires prior authorisation from the CDP. This includes any data relating to genetic data and research in the field of health, data relating to offences, convictions or security measures, processing for the purpose of linkage of files, as well as processing relating to a national identity number or any other general scope identifier, biometric data, or data that has a public interest motive which includes historic, statistical, or scientific purposes. Article 22 specifies what information must be included in a request for such authorisation. Any change in these details must be reported to the CDP, along with any deletion.

The CDP must respond within two months to a request for authorisation or opinion. If not, the request is deemed approved.

Information concerning offences

Processing of data relating to offences, criminal convictions or security measures can only be implemented by courts, public authorities, legal persons managing a public service or court officers.

Health information

Processing of data for health purposes is only legitimate if the data subject has provided consent or has made the data public, and in other specific cases such as if it's necessary to defend their vital interests and they're unable to provide consent, it's necessary to protect public health or prevent a crime, or for preventative or diagnostic medical care. Such data must be collected from the data subject themselves unless it is necessary for the purposes of the processing or if the data subject is not able to provide the data themselves.

Linkage of data

The linkage of data by juristic persons performing a public service for different public interest purposes must be subject to authorisation from the CDP. The same applies to processing implemented by the state for the purpose of making remote services within the framework of electronic administration available to users of the administration. The interconnection of files belonging to private individuals whose main purposes are different, is also subject to authorization by the CDP. Furthermore, it may not lead to discrimination or the reduction of rights, freedoms and guarantees for the data subjects and must be be accompanied by appropriate security measures.

Children

The law does not make mention of specific regulations regarding children.

Direct marketing

Direct marketing is defined as “any solicitation made by sending a message, whatever the medium or the nature including commercial, political or charitable, intended to promote, directly or indirectly, goods, services or the image of a person selling goods or providing services”.

The LDCP prohibits the implementation of direct marketing using any means of communication that uses, in any form whatsoever, the personal data of a natural person who has not expressed their prior consent to receive such marketing.

Automated decision-making

Automated processing of identifiable information carried out on behalf of the state, a public entity, local authority or juristic person bound by private law managing a public service is decided by regulatory act[1] after reasoned opinion by the CDP. This kind of processing relates to state security, defence, or public security; law enforcement data; the population census and the processing of other sensitive data such as data that shows racial, ethnic or regional origins, parentage, political, philosophical or religious opinions or trade union membership either directly or indirectly, or which relates to health or sexual life, as well as salaries, pensions, taxes, duties and other settlements.

No court decision involving an assessment of a person's behaviour can be based on automated processing of personal data intended to assess certain aspects of their personality. Similarly, no decision producing legal effects for a person may be taken on the sole basis of automated processing of personal data. Decisions taken in the context of the conclusion or execution of a contract and for which the data subject has been able to present concerns are excluded.

[1] Note: we have been unable to find such a regulatory act.

Transborder data transfers

Responsible parties may not transfer personal data to another country unless that state provides a sufficient level of protection for privacy and fundamental rights and freedoms with regards to the processing of data. Prior to any transborder transfer, the responsible party must notify the CDP. Likewise, before beginning the processing of any data originating from a different country, the CDP must verify that the responsible party ensures a sufficient level of protection for privacy, rights and freedoms.

A *sufficient level of protection* is determined based on the security measures applied, the specific characteristics of the processing, such as its purposes and duration, and its origin and destination. The CDP may authorise a transfer to a country without a sufficient level of protection if the responsible party provides adequate guarantees to protect the privacy, rights and freedoms of data subjects.

Exceptions: the prohibition is lifted if the transfer is, once-off, minimal and the data subject has provided express consent. Transfer is also permitted if it is necessary to protect a data subject's life or the public interest, to ensure the recognition, exercise or defence of a legal right, or for the performance of a contract between the responsible party and the data subject or pre-contractual measures taken at their request.

Requirements for consent

The LDCP defines consent as any manifestation of will that is express, unequivocal, free, specific and informed by which the data subject or their legal, judicial or contractual representative accepts that their personal data may be processed manually or electronically.

The processing of personal data is only legitimate if the data subject provides their consent, subject to the following exceptions:

- ***Compliance with a legal obligation:*** the processing is necessary to comply with a legal obligation which the responsible party is subject to;
- ***Public interest:*** processing is necessary for the execution of a public interest objective or within the exercise of public authority;
- ***Performance of a contract***: processing is necessary for the performance of a contract to which the data subject is party, or for the execution of pre-contractual measures taken at their request;
- ***Interests, rights and freedoms:*** processing is necessary to safeguard the interests or fundamental rights and freedoms of the data subject.

Transparency

Openness

Article 37 of the law notes that the principle of transparency includes the mandatory provision of information by the responsible party.

Notification of a data breach

The law does not make mention of notification procedures in the event of a data breach.

Impact assessments

The law does not require impact assessments.

Data processing registers

The CDP maintains a directory of personal data processing that is accessible, at no cost, to the public at the Commission's offices or by request to the Commission. This does not include information concerning state security, defence or public security).

Terms of service icons

The law does not mention terms of service icons.

Additional transparency obligations

- ***Publication by the CDP***: the CDP is required to publish all authorisations granted and opinions issued in the directory of processing of personal data.
- ***CDP report:*** the CDP is required to produce an annual activity report to be submitted to the President of the Republic and the President of the National Assembly. The LDCP does not stipulate whether the report is accessible to the public.
- ***Publication of CDP deliberations:*** Decree No. 2008-721 prescribes that deliberations by the CDP must be published in the official journal.

Participation

Data subject participation

Chapter IV covers the rights of data subjects to participate in decisions concerning their personal data. It provides for the following:

- ***Access to personal information:*** any natural person has the right to be informed of that their data is being processed, the right to contest the processing of their data and the right to access their data.

- ***Correction or deletion:*** any natural person has the right to require a responsible party to correct, complete, update, lock or delete personal data concerning them, which is incorrect, incomplete, ambiguous, out of date or illegally collected or processed.

Policy participation

The CDP has the responsibility of presenting suggestions to government to simplify or improve the legislative and regulatory framework with regard to the processing of personal data, as well as to cooperate with data protection authorities from other countries and participate in international negotiations relating to the protection of personal data.

Enforcement

Supervisory authority

The LDCP establishes the Commission for the Protection of Personal Data (CDP). The CDP is an independent administrative authority responsible for ensuring that the protection of personal data is implemented in accordance with the provisions of the LDCP. It informs data subjects and responsible parties of their rights and obligations and ensures that technology does not pose a threat to public freedoms and private life.

Some of the CDP's responsibilities include:

- Inform data subjects and responsible parties of their rights and obligations;
- Receive declarations and requests for authorisation prior to the processing of personal data;
- Receive complaints and provide updates to the complainants;
- Inform the public prosecutor immediately of any infractions it becomes aware of;

- Carry out checks on any processing and obtain copies of documents or information necessary for its duties;
- Impose sanctions on responsible parties, per the provisions in Articles 29 to 32. It may also issue a warning to a responsible party or a formal notice to cease breaches within a specific timeline, which it can block temporarily or permanently;
- Maintain a directory of the processing of personal data which must be made available to the public;
- Publish authorisations granted and opinions issued in the directory of processing of personal data;
- Produce an annual activity report which must be submitted to the President of the Republic and the President of the National Assembly.

The law states that the CDP can be approached by any person, acting by themselves, through their lawyer or by any other duly authorised natural or juristic person.

Sanctions and decisions taken by the CDP may be appealed to the Council of State.

Criminal offences

Violations are provided for and punished by the Penal Code as well as the Cybercrime Law, per the table below.

Civil remedies

The Law does not provide for civil remedies.

Administrative fines

The Law does not provide specifically for administrative fines beyond those listed in the table below.

Offence	Category	Consequence
Failure to comply with formal notices sent by the CDP (state entities or private entities performing a public service are exempt)	Administrative	Temporary withdrawal of authorisation for a period of 3 months, at the end of which the withdrawal becomes final, and/or a fine of 1,000,000 to 100,000,000 Francs CFA
Processing personal data without having complied with the formalities prior to their implementation, even negligently	Criminal	Imprisonment for a term of 1 year to 7 years and/or a fine of 500,000 to 10,000,000 francs
Failure to abide by a formal notice of the CDP, even negligently	Criminal	Imprisonment for a term of 1 year to 7 years and/or a fine of 500,000 to 10,000,000 francs
Failure to comply with the simplified standards or exemptions established by the CDP for common forms of data processing, even negligently	Criminal	Imprisonment for a term of 1 year to 7 years and/or a fine of 500,000 to 10,000,000 francs
Illegal processing of personal data outside the provisions of the law	Criminal	Imprisonment for a term of 1 year to 7 years and/or a fine of 500,000 to 10,000,000 francs
Processing of personal data without implementing the security measures prescribed by the LDCP	Criminal	Imprisonment for a term of 1 year to 7 years and/or a fine of 500,000 to 10,000,000 francs
Collecting personal data by fraudulent, unfair or illegal methods	Criminal	Imprisonment for a term of 1 year to 7 years and/or a fine of 500,000 to 10,000,000 francs
Processing of personal data despite the data subject's objections, if the processing is for advertising purposes, particularly commercial, or if the objection is founded on legitimate reasons	Criminal	Imprisonment for a term of 1 year to 7 years and/or a fine of 500,000 to 10,000,000 francs
Placing or storing sensitive personal data on a computer medium or memory, without the express consent of the data subject, for non-automated processing	Criminal	Imprisonment for a term of 1 year to 7 years and/or a fine of 500,000 to 10,000,000 francs

Placing or storing personal data relating to offences, convictions or security measures on a computer medium or memory outside the provisions of the law	Criminal	Imprisonment for a term of 1 year to 7 years and/or a fine of 500,000 to 10,000,000 francs
Processing personal data for research in the field of health without prior notification to the data subjects of the details of the processing and of their rights to access, to correct and to object to such processing	Criminal	Imprisonment for a term of 1 year to 7 years and/or a fine of 500,000 to 10,000,000 francs.
Processing personal data for research in the field of health without obtaining the express and clear consent of the data subject or their heirs prior to processing	Criminal	Imprisonment for a term of 1 year to 7 years and/or a fine of 500,000 to 10,000,000 francs
Retaining or processing data for longer than necessary, unless for historical, statistical or scientific purposes.	Criminal	Imprisonment for a term of 1 year to 7 years and/or a fine of 500,000 to 10,000,000 francs
Diverting personal data from its purpose as defined by legislative provision, regulatory act, the decision of the CDP, or the prior declaration or authorisation received	Criminal	Imprisonment for a term of 1 year to 7 years and/or a fine of 500,000 to 10,000,000 francs
Sharing personal data with an unauthorised third party, the disclosure of which would have the effect of undermining the consideration of the data subject or their privacy. Prosecution can only be brought on the complaint of the victim, their legal representative or dependents	Criminal	Imprisonment for a term of 1 year to 7 years and/or a fine of 500,000 to 10,000,000 francs
Sharing personal data with an unauthorised third party which undermines the consideration of the data subject or their privacy and it is done recklessly or negligently.	Criminal	Imprisonment for a term of 6 months to 5 years and/or a fine of 300,000 to 5,000,000 francs

Prosecution can only be brought on the complaint of the victim, their legal representative or dependents		
Hindering the action of the CDP by opposing the work of its officers, refusing to provide documents, concealing them, or making them disappear, or by providing incorrect, misleading or inaccessible information	Criminal	Imprisonment for a term of 6 months to 2 years and/or a fine of 200,000 to 1,000,000 francs

SEYCHELLES

As at 20 September 2020

COUNTRY OVERVIEW			Ref
Is there a comprehensive data protection law?	☒	Data Protection Act 9 of 2003 (DPA), not yet in force.	Law link
Does the law establish a supervisory authority?	☒	The DPA establishes the Data Protection Commissioner	S4
Does the law define the term "personal information"?	☒	The term "personal data" is defined in section 2 of the DPA but it does not outline the type of information it includes.	S2(7)
Does the law prohibit the processing of certain types of personal information?	☐	No.	N/A
Does the law prescribe its scope of application?	☐	The law does not prescribe its scope of application but does explicitly note that it applies to public authorities.	S44
Does the law apply extra-territorially?	☐	No.	S45
Does the law set out conditions for the lawful processing of personal information?	☒	The DPA contains eight principals for the lawful processing of personal information.	S3
Does the law stipulate the requirements for valid consent?	☐	No.	N/A
Does the law require opt-in consent?	☐	No.	N/A
Does the law require notification in the event of a data breach?	☐	No.	N/A
Can personal information be transferred to a third party in a foreign country?	☐	As a general principle, the DPA requires that the Data Commissioner be provided with information concerning the transfer of personal data to a third country, and such transfer may be prohibited.	S16
Does the law require a data protection impact assessment to be conducted?	☐	No.	N/A
Does the law require data processing registers?	☒	Yes.	S8
Does the law prescribe the use of terms of service icons or an	☐	No.	N/A

equivalent measure to inform consent of data use?			
Does the law prescribe penalties for non-compliance?	☒	The DPA provides for criminal and civil penalties for non-compliance.	S26

LEGAL ANALYSIS

Legal framework

The Data Protection Act, 2002 (DPA) was enacted in 2003 but has yet to come into force. Section 1 notes that it will come into operation on a date published by the Minister in the Gazette.

There is no additional subsidiary legislation, but the Minister is empowered to make regulations.

Key definitions

The DPA does not have a provision which explicitly notes its scope of application, but the definitions for the key role players, as defined in section 2, include the following:

- The term ***"data subject***" means an individual who is the subject of personal data.

- The term "***data user"*** means a person who holds data. A person is defined to 'hold data' if the following apply:

  (a) "The data forms part of a collection of data processed or intended to be processed by or on behalf of the person mentioned in the definition of 'data'." The definition of 'data' does not explicitly mention a person but, it is assumed that this refers to the person who provides instructions.
  (b) "That person (either alone or jointly in common with other persons) controls the contents and use of the data comprised in the collection, and
  (c) The data are in the form in which they have been or are intended to be processed as mentioned in paragraph (a) or (though not for the time being in that form) in a form into which they have been converted after being so processed and with a view to being further so processed on a subsequent occasion."

- The term "***computer bureau***" is defined to include a person who provides other people with services in respect of data. A person will be considered to do so if –
  (a) As an agent for other persons he causes data held by them to be processed as mentioned in subsection 5 (this subsection provides for the definition of "data"'); or
  (b) He allows other persons the use of equipment in his possession for the processing as mentioned in that subsection of data held by them.

The following definitions are also of relevance:

- The term "***personal data"*** means data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user), including any expression of opinion about the individual but not any indication of the intentions of the data user in respect of that individual.

- The term "***data***" means information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose.

- The term "***processing***" is defined in relation to data, to mean:

  "amending, augmenting, deleting or re-arranging the data or extracting the information constituting the data and, in the case of personal data, means performing any of those operations by reference to the data subject."

Scope of application

The DPA does not have a provision which outlines its explicit scope of application. Section 3(2) notes that there are eight data protection principles; the first seven apply to personal data held by data users and the eighth applies to data and personal data held by persons carrying on computer bureaux. Both data user and computer bureau are defined, but they do not prescribe the bodies which the DPA applies to and it is accordingly unclear whether it applies to natural and juristic persons.

Section 44 prescribes that Public Authorities are subject to the same obligations and liabilities under the Act as private persons. Public authorities are defined to include a Ministry, department, division or agency of the Government, a statutory corporation or a limited liability company. Private persons are not defined in the DPA.

Section 45 notes that the DPA does not apply to a data user or person carrying on a computer bureau where data is held or the service is provided outside of Seychelles. To hold data is defined with reference to section 2(9)(b) which does not exist; it is assumed that the correct reference is 2(10)(b) which requires the data form part of a collection of processed data or data which is intended to be processed. The service is provided outside of Seychelles if the computer bureau either holds data or controls the contents and use of the data in the collection. If a person who is not a resident in Seychelles holds data or provides a service through a servant or agent in Seychelles, then the DPA applies.

The DPA explicitly notes that it does not apply to data processed wholly outside Seychelles unless the data are used or are intended to be used in Seychelles. It is unclear what 'use' entails.

What information does the law apply to?

The DPA applies to personal data which consists of information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user). This includes any expression of opinion about the individual but not any indication of the intentions of the data user in respect of that individual. The definition of personal data excludes data concerning a juristic person.

The DPA does not explicitly note whether it only applies to Seychelles citizens, its scope of application is accordingly unclear in this regard.

Compliance by data users

Data users are obligated to comply with all eight data protection principles. The Definition of data users does not note which bodies may constitute a data user.

Compliance by computer bureaux

The DPA applies to persons carrying on a computer bureau as defined in section 2. Importantly, not all of the principles for the protection of personal data apply to computer bureaux – only principle eight which requires the use of appropriate security measures to guard against loss or destruction of data applies.

Section 19 places an additional obligation on computer bureaux by requiring that they may not disclose personal data without prior authorisation of the data user. Intentionally or recklessly contravening this section constitutes an offence.

Exclusions

The DPA provides for certain exclusions from its scope of application. The exclusions are not absolute, they exempt application to several sections of the DPA, and include the following:

- ***National Security:*** this section notes that personal data is exempt from Part II (regulation of data users and computer bureaux), sections 28 to 31 (Rights of Data Subjects) and sections 9(2)(d) and 19 (non-disclosure) if it is required by national security. This determination will be decided by the Minister and a signed certificate from the Minister is conclusive proof that it was required for national security. The DPA does not define national security or prescribe the considerations to be taken into account by the Minister.

- ***Crime and taxation:*** if personal data is held for the prevention of crime; the apprehension or prosecution of offenders, the collection of any tax or duty or to discharge statutory functions then it is exempt from section 28 and certain provisions of Part II (subject access provisions).

- ***Health and social work:*** the Minister is empowered to exempt personal data consisting of information about the physical or mental health of data subjects from certain provisions by order. She may do so if the data is held by government departments, voluntary organisations or other bodies and it is acquired in the course of carrying out social work.

- ***Regulation of financial services:*** the Minister may exempt certain functions which protect members of the public from financial loss caused by dishonesty, incompetence or malpractice in professional services such as banking, insurance or investment.
- ***Appointments and professional privilege:*** if personal data is held to make government appointments, or if legal privilege applies to the data then it is exempt from section 28 and certain provisions of Part II (subject access provisions).

- ***Payroll and accounts:*** if data is held to calculate remuneration, business accounts, or for the distribution of articles, information or services to data subjects then it is exempt from the subject access provisions. The exemption is conditional on the data not being used for any other purpose but will still apply if it is proven that reasonable care was taken to prevent it from being used for another purpose.

- ***Domestic or other limited purposes:*** if personal data is held to manage personal, family or household affairs then it is exempt from Part II (regulation of data users and computer bureaux) and sections 28 to 31 (rights of data subjects). It also applies to an unincorporated members' club in certain circumstances. If personal data is held only for statistics or research it is exempt from the subject access provisions if they are used only for that purpose, and not published in a form which identifies a data subject.

- ***Examination marks:*** the DPA amends the operation of section 28 (right of access) for data held to determine the results of an academic or professional examination to extend the period to 40 days after the announcement of the marks.

- ***Other exemptions:*** the DPA specifies other circumstances which may warrant an exemption, some of which include a legal requirement that data be made public; data which is subject to a prohibition or restriction or data used for replacement.

Rights of data subjects

The DPA provides a data subject with several rights, they include:

- ***Access:*** the right to be informed whether a data user holds data concerning the data subject and a right to access it. This includes the provision of an explanation where data is expressed in an unintelligible way.

- ***Compensation for inaccuracy:*** if a data subject suffers damage due to the inaccuracy of personal data they are entitled to receive compensation for damage or distress. Data will be considered inaccurate if it is incorrect or misleading. It is a defence to prove that reasonable care was taken in the circumstances to ensure the accuracy of the data.

- ***Compensation for loss or unauthorised disclosure:*** a data subject is entitled to claim damages from a data user or computer bureau for the loss of their personal data, destruction of such data or the unlawful disclosure or access of such data.

- ***Rectification and erasure:*** following an application for compensation for the inaccuracy of personal data, a court may order the rectification or erasure of data. A court is further empowered to order that data be supplemented with true facts. Erasure may be ordered, following a claim for damages due to unlawful disclosure or access of personal data, if there is a substantial risk of further disclosure.

Conditions for the lawful processing of personal information

The DPA prescribes eight principles for the lawful processing of personal data. Principles 1 – 8 apply to data users and principle 8 applies to computer bureaux. Part II of the Act includes an interpretation section which provides additional detail for some of the principles.

- ***The First Principle:*** personal data must be obtained and processed fairly and lawfully. The interpretation notes that regard must be had to the method used to obtain such data and whether it involved deception.

- ***The Second Principle***: personal data may only be held for specified and lawful purposes. The interpretation notes that the purpose must be specified in the data protection register.

- ***The Third Principle:*** personal data must not be used or disclosed in a manner incompatible with its purpose. The interpretation section does not provide additional detail on this principle.

- ***The Fourth Principle:*** pdata held for any purpose must be adequate, relevant and not excessive in relation to its purpose. The interpretation section does not provide additional detail on this principle.

- ***The Fifth Principle:*** personal data must be accurate and kept up to date. The interpretation section notes that it must be determined for the purposes of section 29 which deals with compensation for inaccuracy.

- ***The Sixth Principle:*** personal data must not be kept for longer than required for its purpose. The interpretation section does not provide additional detail on this principle.

- ***The Seventh Principle:*** an individual is entitled to be informed, at reasonable intervals, whether their personal data is being held, to access such data and to have it corrected or erased. The interpretation of this principle considers correction or erasure of personal data to be appropriate only if it is necessary to ensure compliance with other data protection principles.

- ***The Eighth Principle:*** appropriate security measures must be taken to mitigate against unauthorized access, alteration, disclosure or destruction of personal data. The interpretation notes that regard must be had to the harm that may result as well as the storage and access of such data.

The DPA empowers the Minister to modify or supplement the above principles to provide additional safeguards concerning personal data related to: racial origin; political, religious or other beliefs; physical, mental health or sexual life or criminal convictions.

Restrictions on the processing of personal information

Special personal information

The DPA does not prohibit the processing of special categories of data. Section 3(3) empowers the Minister to supplement the data protection principles to provide additional safeguards for information which relates to race, political or religious beliefs, physical and mental health, sexual life and criminal convictions. To date, no supplementary regulations have been published.

Children

The DPA does not include provisions concerning the personal data of children.

Direct marketing

The DPA does not include provisions concerning direct marketing.

Automated decision-making

The DPA does not include provisions concerning automated decision making.

Transborder data transfers

The DPA does not prohibit the transborder transfer of data as the default position subject to exceptions. Instead, it requires that data users specify the list of countries it intends to transfer the data to when applying for registration. If the Commissioner is satisfied that a transfer will contravene one of the data protection principles it may prohibit such transfer. The Commissioner does so by serving a transfer prohibition notice which either prohibits the transfer indefinitely or suspends it until the data user or computer bureaux complies with specified steps.

In deciding whether to issue such a notice, the Commissioner must consider whether doing so will prevent damage or distress and must consider the desirability of the free flow of information. Data users and computer bureaux are given a right to appeal the decision and the Commissioner may cancel the notice at any time.

Such a notice does not prohibit the transfer of data when such transfer is authorised by an enactment which places an international obligation on Seychelles.

Contravention of a transfer prohibition notice is an offence, but it is a defence to prove that due diligence was exercised to avoid contravening the notice.

Requirements for consent

The DPA does not note the requirements for consent.

Transparency

Openness

Openness is not recognized as one of the data protection principles. The seventh principle, however; places an obligation on data users to inform individuals that they hold their data and allow them to access such data.

Notification of a data breach

The DPA does not require that notice be provided for a data breach.

Impact assessments

The DPA does not require the completion of an impact assessment.

Data processing registers

The DPA prescribes that data users and persons carrying on a computer bureau must register with the Commissioner. The holding of personal data is prohibited until their details are contained in the register, the contravention of which is an offence.

The DPA specifies the details which must be included in the registry entry, these include:

- Particulars of the data user;
- A description of the personal data and the purpose of holding or using it;
- A list of the sources from whom the data will be collected;
- A list of the persons to whom the data will be disclosed;
- A list of the foreign countries the data subject intends to transfer the data to;
- One or more addresses for data subject to direct their requests for access to their data.

An entry of a computer bureau is only required to contain the name and address of the person.

A person is prohibited from using data in ways that are not explicitly noted in the register. They are prohibited from transferring the data to additional countries or from obtaining data from sources not listed in their entry. They may not hold or use the data for any purpose other than those specified, or disclose it to persons not detailed in the register.

A person may apply to the Commissioner at any time to alter the particulars contained in the register. The Commissioner is empowered to refuse or accept applications for registration or alteration and must notify the applicant within 6 months. The DPA prescribes that an application must be refused if the particulars don't provide sufficient information or if the Commissioner is satisfied that the applicant is likely to contravene any of the data protection principles. The applicant must be notified if the application is refused and must be made aware of the right to appeal.

The Commissioner is obligated to provide facilities for the public to view the register upon payment of a prescribed fee. Members of the public may request a certified copy of any entry.

Terms of service icons

The DPA does not require the use of terms of service icons.

Additional transparency obligations

The DPA provides for the following which may serve to enhance transparency:

- ***Dissemination by the Commissioner:*** there is an obligation on the Commissioner to disseminate information to the public concerning matters which it thinks are expedient.

- ***Commissioner Report:*** the Commissioner must provide the Minister with an annual report concerning its functions. The DPA does not explicitly provide for the publication of this report or note whether it is accessible by the public.

Participation

Data subject participation

The seventh data protection principle concerns data subject participation. It provides for the following:

- ***The Seventh Principle:*** an individual is entitled to be informed, at reasonable intervals, whether their personal data is being held, to access such data and to have it corrected or erased. The interpretation of this principle considers correction or erasure of personal data to only be appropriate if it is necessary to ensure compliance with other data protection principles. The interpretative provisions note that when determining whether access is requested at reasonable intervals, regard must be had to the nature of the data, the purpose for holding it and the rate at which it is altered.

- ***Access:*** data subjects have a right to be informed whether a data user holds data concerning the data subject and a right to access it. This includes the provision of an explanation where data is expressed in an unintelligible way. Access requires the payment of a prescribed fee, and separate applications must be made for every entry in the register. The data user does not have to comply if doing so would entail disclosing identifiable information relating to another individual, including the source of such data. There is, however, an obligation on data users to supply the information in a way that avoids disclosing the identity of a third party. A data subject may approach a court if the data user has failed to comply with such a request.

Policy participation

The DPA does not require the Commissioner or any other body to keep up to date with any legislative, policy or technological developments which may impact the protection of personal information.

Enforcement

Supervisory authority

The DPA establishes the Data Protection Commissioner (the Commissioner). Its duties are provided for in section 43 and include the promotion of compliance with the data protection principles. It empowers the Commissioner to consider allegations of contravention of the Act if the complaint raises a matter of substance and was brought without delay. The Act does not specify the circumstances which would constitute a matter of substance. The provision does not prescribe the remedial or enforcement powers of the Commissioner, it simply provides that the Commissioner must notify the complainant of "his consideration and of any action which he proposes to take."

Part II of the DOA – concerning regulation of data users and computer bureaux – notes that, following the acceptance of an application, the Commissioner must maintain a register of data users. The provision further notes the application process for the register, which provides the Commissioner's powers in this regard. The Commissioner is empowered to refuse or accept applications for registration or alteration of the particulars in the register.

Section 14 empowers the Commissioner to serve any registered person with an enforcement notice if she is satisfied that they have contravened any of the data protection principles. Such a notice will specify the steps which must be taken. Importantly, this section is not obligatory - the Commissioner *may* serve such a notice. The DPA specifies that in deciding whether to serve such a notice, the Commissioner must consider whether the contravention has or will cause damage or distress. Such an enforcement notice may be appealed, and the time periods for complying with the notice will be suspended until the finalization of the appeal, unless the Commissioner considers compliance to be urgent.

The Commissioner is empowered to cancel an enforcement notice by providing written notice to the person on whom it was served. The DPA does not prescribe considerations which should be taken into account before doing so, nor does it require notification to any additional parties who may be affected by the decision.

The Commissioner is further empowered to serve a de-registration notice on any registered person if satisfied that they have contravened any of the data protection principles. Such a notice authorizes the Commissioner to remove specified entries from the Register. In deciding whether to issue such a notice, the Commissioner must consider whether it has caused any damage or distress and must be satisfied that compliance with the principles cannot be achieved through an enforcement notice.b Such a notice may be appealed and removal will not occur until finalization of the process, unless deemed urgent by the Commissioner.

The Commissioner may apply to the Supreme Court for a warrant. A warrant will be granted if the Judge is satisfied that an offence has or will be committed or one of the data protection principles has or will be contravened. Such a warrant may authorize the Commissioner to enter premises, search them and to inspect, examine, operate and test any data equipment found on the premises. The Commissioner may further inspect and seize any material found on the premises which may constitute evidence. The DPA specifies the conditions for the execution of a warrant, one of which prescribes that reasonable force may be used if necessary. A warrant may not be used for any communication between an attorney and client and section 22(a) notes that it does not apply to personal data which is exempt from part II. This exclusion is unclear – part II does not contain exclusions.

Criminal offences

Certain offences are created under the DPA. These include holding personal data without entry in the register, unauthorised disclosure by computer bureaux and failure to comply with enforcement or prohibition on transfer notices. Liability on conviction results in a fine not exceeding R 20 000 for every offence.

Section 26 notes that any proceedings for an offence may be instituted by the Commissioner or by the Attorney General. It is unclear whether this section precludes other parties from instituting proceedings.

Civil remedies

The DPA provides data subjects with a right of compensation for the inaccuracy of personal data. If a data subject suffers damage due to the inaccuracy of personal data they are entitled to receive compensation for the damage or distress. Data will be considered inaccurate if it is incorrect or misleading. It is a defence to prove that reasonable care was taken in the circumstances to ensure the accuracy of the data. It is unclear what constitutes 'distress' for this right.

The DPA further provides a right to claim compensation for loss or unauthorised disclosure. A data subject is entitled to claim damages from a data user or computer bureau for the loss of their personal data, destruction of such data or the unlawful disclosure or access of such data. The claim includes damages for any distress caused. It is a defence to prove that reasonable care was taken in the circumstances to prevent the loss, destruction, disclosure or access. There is no fault requirement specified in the DPA.

Administrative fines

The DPA does not provide for administrative fines.

Liabilities of directors

The DPA provides that where an offence has been committed by a body corporate and it is proven that it was committed with the consent or neglect of any director, manager or officer then he will also be liable.

Offence	Category	Consequence
Holding personal data without entry in the register	Criminal	A fine not exceeding R 20 000
Knowingly or intentionally contravening section 9 (prohibition of unregistered holding of personal data)	Criminal	A fine not exceeding R 20 000
Failure to make application for an alteration to the register to reflect a current address	Criminal	A fine not exceeding R 20 000
Intentional or reckless provision of false or misleading information when applying for registration or alteration of registered particulars	Criminal	A fine not exceeding R 20 000
Failure to comply with an enforcement notice	Criminal	A fine not exceeding R 20 000
Failure to comply with a transfer prohibition notice	Criminal	A fine not exceeding R 20 000
Unauthorised disclosure by computer bureaux	Criminal	A fine not exceeding R 20 000
Intentional obstruction of the execution of a warrant	Criminal	A fine not exceeding R 20 000
Failure, without reasonable cause, to provide assistance for the execution of a warrant	Criminal	A fine not exceeding R 20 000
If a data subject suffers damage due to the inaccuracy of personal data they are entitled to receive compensation for the damage or distress	Civil	Damages; an order for rectification or erasure
A data subject is entitled to claim damages from a data user or computer bureau for the loss of their personal data, destruction of such data or the unlawful disclosure or access of such data	Civil	Damages; an order for the erasure of the data

SIERRA LEONE

As at 23 September 2020

Sierra Leone does not have a comprehensive data protection framework.

The ICT and Telecommunications sector is regulated by a set of laws comprising the Telecommunications Amendment Acts of 2015, 2009, 2007, and the Telecommunications Act of 2006, which together establish the National Telecommunications Commission, provide for the licensing and regulation of telecommunications operators, for the promotion of universal access to basic telecommunication services, and fair competition in the sector. Also of relevance is the Right to Access Information Act of 2013 which provides for the disclosure of information held by public authorities.

According to a World Bank report, the government has drafted a Data Protection and Archives and Records Management Bill, but it has not yet been published or passed. In 2019, a National Innovation and Digital Strategy for 2019-2029 was published by the Directorate of Science, Technology and Innovation that included a commitment to develop a data protection framework and to establish a data protection authority. A National Cyber Security and Data Protection Strategy published by the Government of Sierra Leone Cyber Incidence Response Team also includes a commitment to strengthen the legal and regulatory framework for data protection.

SOUTH AFRICA

As at 24 August 2020

COUNTRY OVERVIEW			Ref
Is there a comprehensive data protection law?	☒	Protection of Personal Information Act 4 of 2013 (POPIA).	Law link
Does the law establish a supervisory authority?	☒	POPIA establishes the Office of the Information Regulator.	S39
Does the law define the term "personal information"?	☒	The term "personal information" is defined in section 1 of POPIA.	S1
Does the law prohibit the processing of certain types of personal information?	☒	As a general principle, POPIA prohibits the processing of certain types of personal information, referred to as "special personal information", as well as the personal information of children. This is subject to certain exceptions such as the provision of consent or that it is necessary for compliance with a legal obligation.	Part B; Part C
Does the law prescribe its scope of application?	☒	POPIA applies to both public and private bodies, as well as to both natural and juristic persons. Foreign entities, which are not domiciled in South Africa, must comply if they do more than simply forward personal information through South Africa.	S3
Does the law apply extra-territorially?	☐	No.	N/A
Does the law set out conditions for the lawful processing of personal information?	☒	POPIA contains eight conditions for the lawful processing of personal information.	S4
Does the law stipulate the requirements for valid consent?	☒	In order for consent to be valid, it must be a voluntary, specific and informed expression of will.	S1
Does the law require opt-in consent?	☐	No.	N/A
Does the law require notification in the event of a data breach?	☒	In the event of a data breach of personal information, the Information Regulator and the affected data subjects must be notified as soon as reasonably possible.	S22

Can personal information be transferred to a third party in a foreign country?	☐	As a general principle, POPIA prohibits the transfer of personal information to a third party in a foreign country. This is subject to certain exceptions.	S72
Does the law require a data protection impact assessment to be conducted?	☒	The Regulations published in terms of POPIA require information officers to conduct a data protection impact assessment	Regulations
Does the law require data processing registers?	☐	No.	N/A
Does the law prescribe the use of terms of service icons or an equivalent measure to inform consent of data use?	☐	No.	N/A
Does the law prescribe penalties for non-compliance?	☒	POPIA provides for criminal, civil and administrative penalties for non-compliance.	S100 - 109

LEGAL ANALYSIS

Legal framework

The Protection of Personal Information Act 4 of 2013 (POPIA) was enacted to give effect to the right to privacy by regulating the processing of personal information.

POPIA was signed into law on 19 November 2013, but came into force incrementally. Several sections – namely the definitions, the establishment of the Office of the Information Regulator, and the power of the Information Regulator to publish regulations – came into effect on 11 April 2014. The remaining sections – including the eight conditions for the lawful processing of personal information – came into effect on 1 July 2020.

In terms of section 114 of POPIA, all responsible parties have a one-year grace period to comply with the rights and duties provided for in POPIA, which requires compliance as of 1 July 2021. This grace period may be extended by the Minister of Justice and Correctional Services.

In addition to POPIA, the legal framework further comprises the Regulations Relating to the Protection of Personal Information, 2018 (the Regulations). Moreover, the Information Regulator has published the draft Guidelines on the Registration of Information Officers (the draft Guidelines), which closed for public comment on 16 August 2020.

Key definitions

POPIA applies to the processing of personal information of a data subject, which has been entered into a record by or for a responsible party.

The definitions are set out in section 1 of POPIA. In terms of the relevant role-players, the key definitions include the following:

- The term "***data subject***" means the person to whom the personal information relates.

- The term "***responsible party***" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

- The term "***operator***" means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

The following definitions are also of relevance:

- The term "***personal information***" is defined to mean:

  "information relating to an identifiable, living, natural person, and where its applicable, an identifiable, existing juristic person, including but not limited to –

  (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
  (b) information relating to the education or the medical, financial, criminal or employment history of the person;
  (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person.
  (d) the biometric information of the person;
  (e) the personal opinions, views or preferences of the person;
  (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
  (g) the views or opinions of another individual about the person; and
  (h) the name of the person if it appears with other personal information relating to the person or of the disclosure of the name itself would reveal information about the person".

- The term "***processing***" is defined to mean:

  "any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –

  (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
  (b) dissemination by means of transmission, distribution or making available in any other form; or
  (c) merging, linking, as well as restriction, degradation, erasure or destruction of information".

- The term "***record***" is defined to mean any recorded information, regardless of form or medium. This includes writing on any material and information produced, recorded, or stored by means of computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information.

Scope of application

Requirements for the scope of application

POPIA applies to "the processing of personal information entered in a record by or for a responsible party by making use of automated or non-automated means, provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof; and where the responsible party is domiciled in the Republic or not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic". This raises the following considerations:

- ***Processing of personal information:*** there must be processing of personal information.

- ***Entry into a record:*** the personal information must be entered into a record by or for a responsible party.

- ***Automated or non-automated means:*** it is irrelevant whether the responsible party makes use of automated or non-automated means. Automated means is defined as any equipment capable of operating automatically in response to instructions given for the purpose of processing information. If the personal information is processed by non-automated means, this must form part of a filing system or be intended to form part thereof for POPIA to apply.

- ***Domicile in South Africa:*** it is irrelevant whether the responsible party is domiciled in South Africa, provided that the responsible party makes use of automated or non-automated means in South Africa. POPIA does not apply if those means are only used to forward personal information through South Africa.

What information does the law apply to?

POPIA applies to the personal information relating to an identifiable, living, natural person. Furthermore, where applicable, it also applies to the personal information of an identifiable, existing juristic person.

POPIA does not restrict its scope of application to South African citizens. Rather, POPIA protects the personal information of all data subjects in South Africa, provided that the data subject's personal information is processed by a responsible party who falls within the scope of application of POPIA.

Compliance by responsible parties

All private and public bodies who process personal information must comply with POPIA. This includes members of the public, partnerships and companies which process personal information for the purpose of business. It also includes government departments, as well as any institution which exercises a public power or performs a public function. It also applies to non-governmental organisations and civil society organisations. In sum, all natural and juristic persons must comply with POPIA, unless the processing of personal information falls within one of the exclusions, such as processing for purely personal or household activities.

POPIA applies to all responsible parties domiciled in South Africa. Domicile means that the company was incorporated, established or formed in South Africa. POPIA may also apply to responsible parties not domiciled in South Africa if they record person information in a filing system within South Africa, and the personal information is not just forwarded through South Africa.

Compliance by operators

POPIA also applies to operators that process personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of the responsible party. Specifically, POPIA requires that any operator or personal processing personal information on behalf of a responsible party must process such information only with the knowledge or authorisation of the responsible party, and must treat the personal information as confidential and not disclose it unless required by law on in the course of performing their duties.

POPIA also requires that a responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator establishes and maintains appropriate security measures. The operator is required to notify the responsible party immediately where there are grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person.

Exclusions

POPIA provides for certain exclusions from its scope of application. The exclusions include the following:

- ***Personal or household activity:*** processing of personal information in the course of a purely personal or household activity.
- ***De-identification of personal information:*** personal information that has been de-identified to the extent that it cannot be re-identified again. The de-identification of personal information means to delete any information that identifies the data subject; can be used or manipulated by a reasonably foreseeable method to identify the data subject; or can be linked by a reasonably foreseeable method to other information that identifies the data subject.

- ***National security:*** processing of personal information by or on behalf of a public body which involves national security. This exclusion only applies to the extent that adequate safeguards have been established in legislation for the protection of such personal information.

- ***Law enforcement:*** processing of personal information by or on behalf of a public body, the purpose of which is the prevention, detection, investigation or proof of offences, the prosecution of offenders; the execution of sentences; or security measures. This exclusion only applies to the extent that adequate safeguards have been established in legislation for the protection of such personal information.

- ***Cabinet or an Executive Council:*** the processing of personal information by the Cabinet and its committees, or the Executive Council of a province.

- ***Judicial functions:*** the processing of personal information relating to the judicial functions of a court.

- ***Journalistic, literary or artistic purposes:*** the processing of personal information solely for the purposes of journalistic, literary or artistic expression, to the extent that such exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression. Furthermore, where a responsible party who processes personal information for exclusively journalistic purposes is subject to a code of ethics that provides adequate safeguards for the protection of personal information, such code of ethics will apply to the exclusion of POPIA.

Rights of data subjects

POPIA sets out the following rights of data subjects, which includes the following:

- ***Notification:*** the right to be notified that their personal information is being processed or accessed by an unauthorised person.

- ***Access:*** the right to establish whether a responsible party holds personal information about them and to request access to it.

- ***Correction, destruction or deletion:*** the right to request the correction, destruction, or deletion of their personal information.

- ***Objection:*** The right to object to the processing of their personal information.

- ***Direct marketing:*** the right not to have their personal information processed for direct marketing.

- ***Automated decision-making:*** the right not to be subject to a decision which is based solely on automated processing of their personal information.

- ***Redress:*** the right to submit a complaint to the Information Regulator regarding an interference with their personal information, or to institute civil proceedings regarding an interference with the protection of their personal information.

Conditions for the lawful processing of personal information

POPIA prescribes eight conditions for the lawful processing of personal information. Responsible parties must ensure that they process personal information in accordance with these conditions, which are as follows:

- ***Accountability:*** Condition 1 requires that the responsible party must ensure the conditions for the lawful processing of personal information are complied with at the time of determining the purpose and means of the processing, and during the processing itself.

- ***Processing limitation***: Condition 2 requires that personal information must be processed lawfully and in a reasonable manner, and only if it is adequate, relevant and not excessive given the purpose for which it is processed.

- ***Purpose specification:*** Condition 3 requires that personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party, and should not be retained for longer than is necessary to achieve that purpose.

- ***Further processing limitation:*** Condition 4 requires that the further processing of personal information should be compatible with the purpose for which it was collected.

- ***Information quality:*** Condition 5 requires that the responsible party be required to take steps to ensure the personal information is complete, accurate, not misleading and updated where necessary.

- ***Openness:*** Condition 6 requires that the responsible party take reasonably practicable steps to ensure the data subject is aware of, amongst other things, what personal information is being collected, the source of the information, the purpose for which it is being collected, and the name and address of the responsible party.

- ***Security safeguards:*** Condition 7 requires that the responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures, having regard to generally accepted information security practices and procedures.

- ***Data subject participation:*** Condition 8 requires that data subjects be given the right to enquire whether personal information is held about the data subject, and be provided with the record or a description of the information held. Data subjects may further request a responsible party to correct or delete personal information about them if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.

Restrictions on the processing of personal information

Special personal information

POPIA prohibits the processing of special personal information, subject to certain exceptions. Special personal information includes information relating to a data subject's religious or philosophical beliefs; race or ethnic origin; trade union and political affiliations; biometric information; information relating to their health and sex life; as well as information relating to criminal conduct.

The prohibition on the processing of special personal information does not apply if one or more of the following exceptions is applicable:

- ***Consent:*** the processing is carried out with the consent of the data subject.

- ***Legal right or obligation:*** the processing is necessary for the establishment, exercise or defence of a right or obligation in law.

- ***International public law:*** the processing is necessary to comply with an obligation of international public law.

- ***Historical, statistical or research purposes:*** the processing is for historical, statistical or research purposes. This is further subject to the requirement that the purpose of the processing serves a public interest and the processing is necessary for the purpose concerned; or it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent.

- ***Deliberate publication:*** the information has deliberately been made public by the data subject.

The Information Regulator may authorise a responsible party to process special personal information if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the data subject.

Children

POPIA prohibits the processing of personal information concerning a child, subject to certain exceptions. A child is defined as a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of him- or herself.

The prohibition on the processing of personal information concerning a child does not apply if one or more of the following exceptions is applicable:

- ***Consent:*** the processing is carried out with the consent of a competent person.
- ***Legal right or obligation:*** the processing is necessary for the establishment, exercise or defence of a right or obligation in law.
- ***International public law:*** the processing is necessary to comply with an obligation of international public law.
- ***Historical, statistical or research purposes:*** the processing is for historical, statistical or research purposes. This is further subject to the requirement that the purpose of the processing serves a public interest and the processing is necessary for the purpose concerned; or it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent.
- ***Deliberate publication:*** t he information has deliberately been made public by the child with the consent of a competent person.

The Information Regulator may authorise a responsible party to process the personal information of children if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the child.

Direct marketing

POPIA prohibits the processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, subject to certain exceptions. Direct marketing means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or requesting the data subject to make a donation of any kind for any reason.

The prohibition on the processing of personal information for direct marketing does not apply if one or more of the following exceptions is applicable:

- ***Consent:*** the data subject has given his, her or its consent to the processing. The Regulations in terms of POPIA prescribe the form for written consent that must be submitted if personal information is processed for direct marketing.

- ***Existing customer:*** the data subject is a customer of the responsible party.

Any communication for the purpose of direct marketing must contain the details of the identity of the sender or the person on whose behalf the communication has been sent; and an address or other contact details to which the recipient may send a request that such communications cease.

Automated decision-making

POPIA provides that a data subject may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person. This includes performance at work, creditworthiness, reliability, location, health, personal preferences or conduct.

The prohibition on automated decision-making does not apply if one or more of the following exceptions is applicable:

- ***Contractual provision:*** the decision has been taken in connection with the conclusion or execution of a contract. Furthermore, the request of the data subject in terms of the contract must be met; or appropriate measures must have been taken to protect the data subject's legitimate interests.

- ***Law or code of conduct:*** the decision is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.

The reference to appropriate measures requires that the data subject must be provided with an opportunity to make representations about the decision; and the responsible party must provide the data subject with sufficient information about the underlying logic of the automated processing of information to enable him or her to make such representations.

Transborder data transfers

POPIA prohibits the transfer of personal information about a data subject to a third party who is in a foreign country, subject to certain exceptions.

The prohibition on transborder data transfers does not apply if one or more of the following exceptions is applicable:

- ***Adequate level of protection:*** the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection.

- ***Consent:*** the data subject consents to the transfer.

- ***Performance of a contract:*** the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request.

- ***Conclusion or performance of a contract:*** the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party.

- ***Benefit of the data subject:*** the transfer is for the benefit of the data subject; it is not reasonably practicable to obtain the consent of the data subject to that transfer; and if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

POPIA requires that responsible parties must obtain prior authorisation from the Information Regulator if that responsible party plans to transfer special personal information or personal information concerning a child to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information.

Requirements for consent

Consent is one of the justifications for the lawful processing of personal information. If the data subject is a child, consent must be provided by a competent person. Consent is defined in POPIA to mean "any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information".

A data subject may withdraw consent at any time, provided that the withdrawal will not affect the lawfulness of the processing which occurred before the withdrawal of consent.

The legislative framework does not expressly prohibit discrimination for declining consent.

Transparency

Openness

Condition 6 of the conditions for the lawful processing of personal information pertains to openness. This requires that if personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of relevant information, including the information being collected; the source from which it is collected; the name and address of the responsible party; the purpose for which the information is being collected; whether or not the supply of the information is voluntary or mandatory; the consequences of the failure to provide the information; and any particular law authorising or requiring the collection of the information.

POPIA provides for certain exceptions to compliance with this condition, such as where the data subject has provided consent for the non-compliance; or where non-compliance would not prejudice the legitimate interests of the data subject.

Notification of a data breach

A responsible party is obliged to notify the Information Regulator and affected data subjects when there are reasonable grounds to believe that their personal information has been accessed or acquired by an unauthorised person. The responsible party must provide such notice as soon as reasonably possible after the discovery of the compromise.

The Information Regulator may direct a responsible party to publicise the fact of any compromise to the integrity or confidentiality of personal information, if the Information Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

Impact assessments

The Regulations in terms of POPIA require that a personal information impact assessment be conducted by an information officer to ensure that adequate measures exist to comply with the requirements for the lawful processing of personal information. The legislative framework does not prescribe a timeframe for completion of such an assessment or a requirement that it be published.

Data processing registers

POPIA does not require the creation or publication of a data processing register.

Terms of service icons

POPIA does not require the use of terms of service icons.

Additional transparency obligations

In addition to the above, the following measures may also serve to enhance transparency:

- ***Compliance framework:*** information officers are required to ensure that a compliance framework is developed, implemented, monitored and maintained.
- ***Access to information manual:*** information officers are required to ensure that a manual is developed, monitored, maintained and made available as prescribed by the Promotion of Access to Information Act 2 of 2000.
- ***Data subject access requests:*** information officers are required to ensure that internal measures are developed, together with adequate systems, to process requests for information or access thereto.
- ***Particulars of information officers and deputy information officers:*** the Information Regulator is required to make the contact details of information officers and deputy information officers available on its website.
- ***Reporting by the Information Regulator:*** the Information Regulator is empowered to publish a report relating to any of its functions in terms of POPIA, including cases of non-compliance that have been investigated.

Participation

Data subject participation

Condition 8 of the conditions for the lawful processing of personal information pertains to data subject participation. It provides for the following:

- ***Access to personal information:*** a data subject has the right to request a responsible party to confirm whether or not the responsible party holds personal information about the data subject; and to request the responsible party to provide the record or a description of such personal information.
- ***Correction or deletion of personal information:*** a data subject may request a responsible party to correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.
- ***Destruction or deletion of a record:*** a data subject may request a responsible party to destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised to retain.

On receipt of a request to correct or delete personal information or to destroy or delete a record, the responsible party must, as soon as reasonably practicable, correct the information; destroy or delete the information; provide the data subject, to his or her satisfaction, with credible evidence in support of the information; or where agreement cannot be reached between the responsible party and the data subject, take such steps as are reasonable to attach an indication that a correction of the information has been requested but not made.

Policy participation

The Information Regulator is required to keep up to date with any legislative, policy or technological developments which may impact the protection of personal information, and must further submit a report to Parliament on any necessary action to be taken.

Enforcement

Supervisory authority

POPIA establishes the Office of the Information Regulator, an independent juristic entity that is responsible for monitoring and ensuring compliance with POPIA. The Information Regulator is accountable to the National Assembly of Parliament.

The Information Regulator must provide education; handle complaints; conduct research; and monitor legislative and policy changes which may impact on the protection of personal information.

The Information Regulator is empowered to investigate allegations of violations of the provisions of POPIA and may assess compliance on its own initiative or following the receipt of a complaint. Upon receipt of a complaint, the Information Regulator may conduct a pre-investigation; decide to take no action; conduct a full investigation; act as a conciliator; or refer the matter to the enforcement committee.

If there are reasonable grounds to suspect that a responsible party is interfering with the protection of personal information or that an offence under POPIA has been committed, the Information Regulator may apply for a warrant. A warrant empowers the Information Regulator to enter and search premises and inspect, examine, operate, or test any equipment which is used for the processing of personal information. Furthermore, the Information Regulator may seize any record, material or equipment as evidence.

In the event that a responsible party is found to be interfering with the protection of personal information, the Information Regulator may serve them with an enforcement notice. In such a notice, the Information Regulator can specify steps they must comply with or prohibit them from processing personal information as specified. Non-compliance with such a notice is an offence.

Criminal offences

Certain criminal offences are created under POPIA. These include obstructing or unlawfully influencing the Information Regulator; a breach of confidence by the Information Regulator; the obstruction of the execution of a warrant; and the failure to comply with an enforcement notice or an information notice. There are also various offences relating to witnesses, some of which include the failure to attend as specified in a summons; and the provision of false information. Furthermore, the failure to process information concerning an account number in compliance with POPIA is an offence as well.

Certain contraventions carry a penalty of a fine and/or imprisonment of up to 10 years, while others carry a penalty of a fine and/or imprisonment of up to 12 months.

Civil remedies

A data subject, or the Information Regulator on behalf of a data subject, may institute a civil action for damages for non-compliance with POPIA, regardless of whether non-compliance was negligent or intentional. Such a claim may include the award of an amount for patrimonial loss, non-patrimonial loss and/or aggravated damages.

While POPIA does not expressly provide for class action proceedings, this remains a possibility under South African law.

Administrative fines

If a responsible party is alleged to have committed an offence in terms of POPIA, the Information Regulator may deliver an infringement notice to the responsible party. This notice must specify the name and address of the infringer; the particulars of the alleged offence; and the amount of the administrative fine payable. The infringement notice must also explain that the infringer can pay the administrative fine; make arrangements with the Information Regulator to pay the administrative fine in instalments; or elect to be tried in court on a charge of having committed the alleged offence referred to in terms of POPIA.

The administrative fine may not exceed R10 million (ZAR). When determining an appropriate fine, the Information Regulator must consider the nature of the personal information involved; the duration and extent of the contravention; the number of data subjects affected or potentially affected by the contravention; whether or not the contravention raises an issue of public importance; the likelihood of substantial damage or distress; whether the responsible party or third party could have prevented the contravention from occurring; any failure to carry out a risk assessment or a failure to operate good policies, procedures and practices to protection personal information; and whether the responsible party had previously committed an offence in terms of POPIA.

Offence	Category	Consequence
Hindering, obstructing or unlawfully influencing the Information Regulator	Criminal	A fine or imprisonment not exceeding 10 years, or both
Breach of Confidentiality by the Information Regulator	Criminal	A fine or imprisonment not exceeding 12 months, or both
Obstructing the execution of a warrant	Criminal	A fine or imprisonment not exceeding 12 months, or both
Failure to assist with the execution of a warrant	Criminal	A fine or imprisonment not exceeding 12 months, or both
Failure to comply with an enforcement notice	Criminal	A fine or imprisonment not exceeding 10 years
Concerning an information notice, a Responsible Party provides a statement knowing it to be false	Criminal	A fine or imprisonment not exceeding 12 months, or both
Concerning an information notice, a Responsible Party recklessly makes a statement which is false, in a material respect	Criminal	A fine or imprisonment not exceeding 12 months, or both
Failure to attend at the time and place specified in a summons	Criminal	A fine or imprisonment not exceeding 12 months, or both
Failure to attend, as summoned, until excused	Criminal	A fine or imprisonment not exceeding 12 months, or both
Refusal or failure to make an affirmation as a summoned witness	Criminal	A fine or imprisonment not exceeding 12 months, or both
Failure to adequately respond to a question as a summoned witness	Criminal	A fine or imprisonment not exceeding 12 months, or both
Failure to produce a document as requested in a summons	Criminal	A fine or imprisonment not exceeding 12 months, or both
The provision of false evidence as a witness	Criminal	A fine or imprisonment not exceeding 10 years
Obtaining or disclosing an account number of a data subject	Criminal	A fine or imprisonment not exceeding 10 years
The contravention of lawful processing of an account number, of a persistent nature which is likely to cause damage or distress to the data subject	Criminal	A fine or imprisonment not exceeding 10 years
Interference with the protection of personal information of a data subject through the breach of any of the conditions for lawful processing	Civil	Comply with specified steps; or stop processing personal information as specified; comply with an enforcement notice; civil remedies

Failure to comply with breach notification	Civil	Comply with specified steps; or stop processing personal information as specified; or comply with an enforcement notice; civil remedies
Breach of Confidentiality by the Information Regulator	Civil	Comply with specified steps; or stop processing personal information as specified; comply with an enforcement notice; civil remedies
Failure to comply with conditions for direct marketing	Civil	Comply with specified steps; or stop processing personal information as specified; comply with an enforcement notice; civil remedies
Failure to comply with conditions for Directories	Civil	Comply with specified steps; or stop processing personal information as specified; comply with an enforcement notice; civil remedies
Failure to comply with conditions for automated decision making	Civil	Comply with specified steps; or stop processing personal information as specified; comply with an enforcement notice; civil remedies
Failure to comply with conditions for transborder flows	Civil	Comply with specified steps; or stop processing personal information as specified; comply with an enforcement notice; civil remedies

TUNISIA

As at 18 September 2020

COUNTRY OVERVIEW			Ref
Is there a comprehensive data protection law?	☒	Yes, Law No. 2004-63 of 27 July 2004	Law link
Does the law establish a supervisory authority?	☒	The Law establishes the National Authority for the Protection of Personal Data.	Article 75
Does the law define the term "personal information"?	☒	The term "personal information" is defined in Article 4 of the Law.	Article 4
Does the law prohibit the processing of certain types of personal information?	☒	The Law prohibits the processing of certain types of personal information, referred to as "sensitive personal information", subject to some exclusions. It also states specific processing conditions for data relating to children, health, research and video-surveillance.	Article 14 and Sections II, III and IV
Does the law prescribe its scope of application?	☒	The Law applies to both public and private bodies, as well as to both natural and juristic persons. Persons who are nationals of or resident in Tunisia must comply.	Article 22
Does the law apply extra-territorially?	☐	No.	N/A
Does the law set out conditions for the lawful processing of personal information?	☒	The Law sets out at least 5 conditions for the lawful processing of personal information.	Articles 7 and 8 and Section II
Does the law stipulate the requirements for valid consent?	☐	Not specifically, although it does state certain specific conditions for consent in some provisions.	Articles 14, 27 and 30
Does the law require notification in the event of a data breach?	☐	No.	N/A

Can personal information be transferred to a third party in a foreign country?	☒	Transborder transfer is subject to consent from the Authority and other conditions.	Articles 50, 51 and 52
Does the law require a data protection impact assessment to be conducted?	☐	No.	N/A
Does the law require data processing registers?	☐	No.	N/A
Does the law prescribe the use of terms of service icons?	☐	No.	N/A
Does the law prescribe penalties for non-compliance?	☒	The Law provides for criminal and administrative penalties for non-compliance.	

LEGAL ANALYSIS

Legal framework

Law No. 2004-63 of 27 July 2004 (the Law) was enacted to protect privacy which is one of the fundamental rights guaranteed by the Tunisian constitution. The law is only available in French.

Persons which fall within the scope of application of the law were given one year to comply with its provisions. It wasn't until 2015 that data processors began to regularly declare their personal data processing to the data protection authority, as required by the Law, after the President of the INPDP announced his intention to fully implement the penalties contained in the Law starting 30 September 2015.

In addition to the Law, Decree No. 2007-3004 lays out the conditions and procedures for the declaration and authorisation of the processing of person data to the protection authority, and Decree No. 2007-3003 sets out the modalities for the functioning of the protection authority.

In March 2018, Tunisia introduced a new draft law on the protection of personal data that is in line with the new European GDPR, but it has not yet been enacted.

Key definitions

The definitions are set out in Articles 4 to 6 of the Law. In terms of the relevant role players, the key definitions include the following:

- The term ***"data subject"*** is defined to mean any natural person whose personal data is subject to processing.

- The term ***"responsible party"*** is defined to mean any natural or juristic person who determines the purposes and methods of processing of personal data.

- The term ***"subcontractor"*** is defined to mean any natural or juristic person who processes personal data on behalf of a responsible party.

- The term ***"recipient"*** is defined to mean any natural or juristic person who receives personal data.

- The term ***"third party"*** is defined to mean any natural or juristic person, public authority or its subordinates, other than the data subject, the recipient, the responsible party, the sub-contractor or their subordinates.

- The term ***"the Authority"*** means the National Authority for the Protection of Personal Data.

The following definitions are also of relevance:

- The term ***"personal data"*** is defined to mean all information regardless of its origin or form and which directly or indirectly enables a natural person to be identified or makes them identifiable, with the exception of information related to public life or considered as such by law. The term "identifiable" means that a natural person is likely to be identified, directly or indirectly, through several data or symbols which concern in particular their identity, their physical, physiological, genetic, psychological, social, economic or cultural characteristics.

- The term ***"processing of personal data"*** is defined to mean operations carried out in an automated or manual manner by a natural or juristic person, and whose purpose in particular is the collection, recording, conservation, organisation, modification, use, dispatch, distribution, dissemination, destruction or consultation of personal data, as well as all operations relating to the use of databases, indexes, directories, files, or linking.

Scope of application

Requirements for the scope of application

The Law applies to the processing of personal data, whether automated or non-automated, implemented by natural or juristic persons. This raises the following considerations:

- ***Processing of personal information:*** there must be processing of personal information.

- ***Automated or non-automated means:*** it is irrelevant whether the responsible party makes use of automated or non-automated means

The Law also stipulates that if any natural person or legal representative of a juristic person wishes to process personal data, they must meet the following conditions:

- Be of Tunisian nationality;
- Be resident of Tunisia;
- Be without a criminal record.

What information does the law apply to?

The Law applies to the processing of all personal data, whether automated or not, by natural or juristic persons. The Law specifies that data processed by Tunisian nationals or residents of Tunisia fall within its scope of application, but it does not provide further detail.

Compliance by responsible parties

All natural and juristic persons, including public and private bodies, who process data must comply with the Law, unless they fall within one of the exclusions. The Law does not explicitly note whether juristic persons must be domiciled in Tunisia, but Article 22 states that any legal or juristic person wishing to process personal data, or their agents, must be of Tunisian nationality and resident in the country.

Compliance by sub-contractors

The responsible party is required to scrupulously choose a sub-contractor. Processing must be mandated by contract and the sub-contractor is bound by the same obligations as responsible parties. The subcontractor must respect the provisions of the Law and may not act outside the limits authorised by the responsible party.

Exclusions

The Law does not apply to the following types of data processing:

- ***Personal or household activity:*** the law does not apply to the processing of personal data for solely personal or family use, provided it is not transmitted to third parties;

- ***Employment information***: data concerning an employee's professional situation does not require prior declaration or authorisation, consent, or data subject notification and is not subject to the restrictions on transfer. This exclusion applies if the processing is carried out by the employer and is necessary for the functioning of the organisation;

- ***Processing by public entities:*** public entities are exempt from the provisions on declarations or authorisations, consent, children, the right to object, and the provisions on collecting data directly from data subjects. Data subjects do not have the right to access data processed by public entities, but may request correction or deletion if they are aware of errors. Furthermore, public entities may not communicate data to private entities without the data subjects' consent.

Rights of data subjects

Section III of the Law sets out the rights of data subjects, which include the following:

- ***Consent:*** data processing may only occur with the express and written consent of the data subject. If a data subject is incapable or prohibited from providing consent, then the general rules of law concerning consent apply. A data subject may retract their consent at any time. Consent is not required if it is evident that the processing is carried out in the data subject's interest and contacting the data subject is impossible, if obtaining their consent implies disproportionate efforts, or if the processing of personal data is provided for by law or an agreement to which the data subject is party. Consent applies only to the specific data processing purpose for which it was given.

- ***Notification:*** after expiry of the period for submitting declarations to the Authority and if no objection has been received, the responsible party must provide prior written notification to the data subject of the collection of their personal data within at least one month of the processing starting. Information must provided concerning the purposes for which it is being collected, the nature of the data, whether their response is obligatory, the consequences of a default response, details of the responsible party and the data subject's rights, the duration of retention and a description of the security measures being taken to protect the data.

- ***Access:*** a data subject has the right to consult all personal data concerning them and to obtain a copy in clear language and in an intelligible form if they are processed with the aid of automatic processes, free of charge. The right to access cannot be waived beforehand, but may be limited if the data is being processed for scientific purposes that do not substantially affect the data subject's privacy or if it is to protect the data subject or a third party.

- ***Correction or deletion***: a data subject has the right to correct, complete, rectify, update, modify, clarify or erase data relating to them if it is inaccurate, ambiguous, or their processing is prohibited.

- ***Objection:*** data subjects have the right to oppose processing of their personal data at any time for valid, legitimate, and serious reasons. The Law does not stipulate what would constitute such a reason. Similarly, they have the right to object to their data being communicated to third parties for advertising purposes. Stating an objection immediately suspends the processing of the data.

Conditions for the lawful processing of personal information

Before processing personal data, a responsible party must submit a declaration to the Authority. The conditions and procedures for making such declarations are defined in Decree No. 2007-3004. A receipt or any other means of written acknowledgement of receipt must be received before processing can begin. If no confirmation is received from the Authority within one month, acceptance can be inferred.

Processing of certain types of personal data further requires prior authorisation from the Authority. Article 8 specifies the information which must be included in a request for authorisation, some of which include the purpose of the processing, the origin of the data and the security measures taken to protect the data. Re-authorisation must be obtained for any changes to these details. If no response is received on a request for authorisation within 30 days, it is deemed to be refused. The Authority may provide conditional approval which is subject to compliance by the responsible party with specified safeguards necessary to protect the interests of data subjects.

Responsible parties must ensure that they process personal information in accordance with these conditions, which are as follows:

- ***Purpose Specification:*** the collection of personal data must be carried out for lawful, defined and explicit purposes. Processing may not be carried out for different purposes unless the data subject has provided consent, it is necessary to protect their vital interests, or for certain scientific purposes.

- ***Processing limitation:*** personal data must be treated fairly and processed only to the extent necessary for the purposes for which it was collected.

- ***Information quality:*** the responsible party must ensure that the data is exact, accurate and up to date. If the data is inaccurate or insufficient, both the responsible party and the subcontractor must correct, complete, modify, update, or erase the files at their disposal. They must also inform the data subject and any legitimate data recipient of any modifications made within two months.

- **Security safeguards:** any person implementing data processing must take all necessary precautions to ensure the security of the data and to prevent third parties from modifying, altering or consulting the data without the authorisation of the data subject. The detailed security precautions that are necessary are provided in Article 19.

- ***Retention period limitation:*** data must be destroyed after the period stated in the declaration or authorisation has expired, if the purpose for which it was collected has been achieved, or if the data is no longer useful for that purpose. To destroy data, a report is drawn up by a bailiff in the presence of an expert appointed by the Authority, at the cost of the responsible party. Personal data communicated or likely to be communicated to public entities may only be destroyed after obtaining the opinion of those entities as well as the authorisation of the Authority, which must be given within one month.

Some additional requirements also apply. These include the following:

- ***Direct collection:*** personal data may only be collected directly from data subjects, unless they have provided consent, subject to certain exceptions. Consent is not required if obtaining it entails "disproportionate effort" or if the collection does not manifestly affect the data subject's legitimate interests.

- ***Conditional service***: it is strictly prohibited for the provision of a service or approval of a benefit to be conditional upon a person's acceptance of the processing of their personal data or their acceptance of it being used for purposes beyond those which it was collected for.

- ***Transfer to third parties:*** the Law prohibits the transfer of personal data to third parties without the express, written consent of the data subject, unless the data is necessary for public security or national defence, or for the implementation of criminal proceedings. The Authority may authorise the transfer of data even if the data subject has refused to consent if it protects their vital interests, is used for research or historical or scientific studies, or is necessary for the execution of a contract to which the data subject is part. In such an instance, the recipient of the data must implement appropriate security guarantees to protect the data.

- ***Confidentiality***: responsible parties, subcontractors and their agents must preserve the confidentiality of the data. They are obligated to do so even after the end of processing or a decline in their quality, unless the distribution of the data has been accepted in writing by the data subject or provided for by law.

- ***Processing ceases***: if a responsible party wishes to permanently cease their data processing activities, they must inform the Authority three months before the date of cessation. In the case of death, bankruptcy or dissolution of the responsible party, the heirs, bankruptcy trustee or liquidator must inform the Authority within three months, following which the Authority has one month to authorise the destruction of the personal data concerned. Alternatively, the Authority may authorise transfer of the data if it judges it to be useful for historical or scientific purposes, or if the original responsible party identifies another to whom they will transfer the data, provided the Authority agrees and the data subject has given written consent. If the data subject does not agree, the data must be destroyed within three months. Lastly, in such cases the data subject, their heirs, any

interested person of the public minister may request the Authority to retain the data or to destroy it. For cases relating to data processed by public entities, the Authority is responsible for conserving, protecting or destroying the data.

Restrictions on the processing of personal information

Special personal information

The Law prohibits the processing of data related to offences, their ascertainment, criminal proceedings, penalties, preventative measures or criminal records, unless it is carried out by public entities or private entities carrying out a public service.

It is also prohibited to process data relating, either directly or indirectly, to racial or genetic origin, religious convictions, political, philosophical or trade union opinions, or health. This is, however, subject to certain exceptions, such as obtaining a data subject's written consent, if the data has acquired a manifestly public character, for historic or scientific purposes, if the processing is necessary to protect the vital interests of the data subject, or if it is carried out by public entities or private entities carrying out a public service. Processing of this data is subject to authorisation from the Authority, with the exception of health data.

Children

Article 28 states that the processing of a child's personal data may only be carried out after obtaining the consent of the child's guardian or after authorisation by a family judge, who may authorise the processing without the consent of the guardian if the best interests of the child so require. The judge may also revoke their authorisation at any time.

Similarly, the transborder transfer of data relating to children must be presented to a family judge.

Direct marketing

The Law prohibits the processing of personal data for advertising purposes without the express and specific consent of the data subject.

Automated decision-making

The only specification in the Law for automated decision-making concerns the obligation held by responsible parties to ensure the data subject's right to access and to obtain a copy of the data in an intelligible form. This includes implementing the technical means necessary to allow the data subject to send their request for correction or deletion of personal data by electronic means.

Health

Health data may only be processed if one or more of the following conditions applies:

- The data subject has provided consent;
- It is necessary for the exercise of laws or regulations;
- It is necessary for the protection of public health;
- It is beneficial for the health of the data subject;
- It is necessary for preventative or therapeutic reasons for the health of the data subject;
- It takes place in the context of scientific research in the field of health.

It may also only be processed by a doctor or someone who is bound by professional confidentiality. These parties may transfer data to others carrying out scientific research in the field of health with authorisation from the Authority. The Authority may mandate certain precautions or protection measures to be taken to protect the data, or may prohibit the transfer.

Research

Personal data collected for research purposes must not contain elements likely to reveal the identity of the data subject if the requirements of scientific research allow it. The dissemination of such data may only be carried out if the data subject has provided express, written consent or if it is necessary for the presentation of research results relating to events or phenomena existing at the time of the presentation.

Surveillance

Chapter IV of the Law states that the use of video-surveillance tools is subject to authorisation from the Authority. Video-surveillance tools may only be used in the following places and only if they are necessary to ensure the security of people, the prevention of accidents, the protection of goods, or management of the entry and exit of the following places:

- Places open to the public and their entrances;
- Parking spaces, public transport means, stations, maritime ports or airports;
- Places of collective work.

In any case, video recordings cannot be accompanied by sound recordings.

The public must be clearly informed of the existence of the video-surveillance. The Law prohibits the communication of recordings unless the data subject has provided consent, it is necessary for the work of public authorities, or for the recognition, discovery or prosecution of criminal offenses.

Video recordings must be destroyed when they are no longer necessary for the realisation of the purposes for which they were collected, or when the interest of the data subject requires its deletion. This does not apply if the records are required for the investigation and prosecution of criminal offences.

Transborder data transfers

The Law forbids transborder data transfers if it is likely to threaten the public security or vital interests of Tunisia. Transfers may only be allowed if the receiving country provides sufficient protections for the security of the data, and only after receiving authorisation from the Authority. The Law does not stipulate the conditions required for 'sufficient protection'.

Requirements for consent

The Law contains no specific definition of consent, though certain elements are specified in certain provisions. In most cases, consent requires using a method that leave a written record, and requires it to be "express and specific".

Transparency

Openness

Section III Sub-Section II of the Law pertains to openness. This requires that if personal information is collected, the responsible party must take certain steps to ensure that the data subject is aware of relevant information about the data processing. This includes notification concerning the purposes for its collection, the nature of the data, whether their response is obligatory, the consequences of a default response, details of the responsible party, the data subject's rights, the duration of retention and a description of the security measures taken to protect the data.

It also mandates that a data subject has the right to consult all personal data concerning them and to obtain a copy, subject to certain exclusions.

Notification of a data breach

The Law does not provide for procedures for notification in the case of a data breach.

Impact assessments

The Law does not make provision for impact assessments.

Data processing registers

The Law does not make provision for data processing registers.

Terms of service icons

The Law does not make provision for terms of service icons.

Additional transparency obligations

There are no further transparency obligations in the Law.

Participation

Data subject participation

Section III of the Law pertains to data subject participation. It provides for the following:

- ***Access to personal information:*** a data subject has the right to be informed that their personal data is being processed, to consult all personal data concerning them and to obtain a copy in clear language and an intelligible form, free of charge, though this right may be limited in certain situations.

- ***Correction or deletion***: a data subject may request the responsible party to correct or delete data relating to them if it is inaccurate, ambiguous, or their processing is prohibited. The data subject must be informed of any corrections or modifications within two months.

Policy participation

The Authority is mandated to "determine the essential guarantees and appropriate measures for the protection of personal data" as well as provide opinions, develop rules of conduct, and participate in research, training, and study activities.

Enforcement

Supervisory authority

Chapter VI of the law establishes the National Authority for the Protection of Personal Data (INPDP), which has a legal personality and enjoys financial autonomy.

The Authority's responsibilities are as follows:

- Grant authorisations and receive declarations for the processing of personal data, or withdraw them;
- Receive complaints;
- Determine the essential guarantees and appropriate measures for the protection of personal data;
- Carry out investigations, access the personal data being processed, and collect information in order to verify them. The Authority must inform the relevant public prosecutor of all the offences of which it becomes aware in the course of its work;
- Provide opinions on subjects related to data protection;
- Develop rules of conduct relating to the processing of personal data;

- Participate in research, training and study activities related to the protection of personal data, and in general in any activity related to its field of intervention.

If a responsible party or subcontractor refuses to honour a data subject's right to access data concerning them, they may make a request to the Authority within one month of the data of refusal. Within one further month, the Authority is required to make an order regarding access to the data, provision of requested copies, or refusal. A data subject may also make a request for the destruction or concealment of data relating to them, to which the Authority must respond in seven days. In the case of disputes about data quality, access to data, or objections to processing, the responsible party must notify the Authority, which will make a decision within one month. The decisions of the Authority may be appealed to the Tunis Court of Appeal within one month.

The Protection Authority may also decide to withdraw or suspend an authorisation for processing.

Criminal offences

Sanctions are defined in Chapter VII of the Law. Article 97 of the Law also states that Article 254 of the penal code applies to responsible parties, sub-contractors or members of the Authority who divulge the content of personal data outside of the cases provided for in the Law.

In addition to the penalties in the table below, some violations require additional remediation steps to be taken. For example, in the case of a violation of disseminating data which causes harm to the data subject or their privacy, the data subject may ask the court to order the publication of an extract from the judgment in one or more daily newspapers in Tunisia. Prosecutions can only be initiated at the request of the person concerned. Desisting from the dissemination halts the prosecution, the trial or the execution of the sentence. Penal mediation may be carried out in some cases.

When the offender is a legal person, the penalties provided for in the Law are applied personally to the legal or de facto leader of the legal person who is responsible for the acts concerned.

The offences provided for in Chapter VII are recorded by the judicial police officers mentioned in numbers 1 to 4 of article 10 of the Code of Criminal Procedure, and by sworn officers of the ministry in charge of communication technologies

Civil remedies

The Law does not provide for civil remedies.

Administrative fines

The Law provides for administrative fines for certain less serious violations, such as incorrectly receiving data or failing to notify the Authority about disputes.

Offence	Category	Consequence
Violation of provisions relating to transfer of data to a foreign country threatening public security or the vital interests of the state	Criminal	Imprisonment of 2 to 5 years and a fine of 5 000 dinars to 50 000 dinars
Violation of provisions concerning processing of data related to offences, their establishment, criminal proceedings, preventive measures or criminal records	Criminal	Imprisonment of 2 years and a fine of 10 000 dinars
Violation of provisions concerning processing of data relating to racial or genetic origin, religious convictions, political, philosophical or trade union opinions, or health.	Criminal	Imprisonment of 2 years and a fine of 10 000 dinars

Violation of the provisions around processing of children's personal data	Criminal	Imprisonment of 2 years and a fine of 10 000 dinars
Processing of health data by someone other than a doctor or person bound by professional confidentiality	Criminal	Imprisonment of 2 years and a fine of 10 000 dinars
Use of video-surveillance technology in unauthorised places	Criminal	Imprisonment of 2 years and a fine of 10 000 dinars
Violation of the provisions around necessity of use of video-surveillance technology	Criminal	Imprisonment of 2 years and a fine of 10 000 dinars
Violation of consent obligations	Criminal	Imprisonment of 2 years and a fine of 10 000 dinars
Violation of notification obligations	Criminal	Imprisonment of 2 years and a fine of 10 000 dinars
Violation of the provisions relating to the direct collection of data from data subjects except in specific circumstances	Criminal	Imprisonment of 2 years and a fine of 10 000 dinars
Violation of the conditions for the lawful sharing of data for scientific research	Criminal	Imprisonment of 2 years and a fine of 10 000 dinars
Obtaining consent for the use of personal data through fraud, violence or threats	Criminal	Imprisonment of 1 year and a fine of 10 000 dinars
Intentionally communicating data for one's own profit or the profit of another or to cause harm to the data subject	Criminal	Imprisonment of 1 year and a fine of 5 000 dinars
Intentionally implementing processing without presenting a prior declaration or authorisation, or continuing processing after receiving a prohibition from processing	Criminal	Imprisonment of 1 year and a fine of 5 000 dinars
Sharing personal data relating to health despite a prohibition from the Authority	Criminal	Imprisonment of 1 year and a fine of 5 000 dinars

Transferring data to a foreign country without the authorisation of the Authority	Criminal	Imprisonment of 1 year and a fine of 5 000 dinars
Communicating data without the consent of the data subject or the approval of the Authority in cases where it is required	Criminal	Imprisonment of 1 year and a fine of 5 000 dinars
Continuing to process personal data against objections from the data subject	Criminal	Imprisonment of 1 year and a fine of 5 000 dinars
Intentionally limiting or hindering exercise of the right to access	Criminal	Imprisonment of 8 months and a fine of 3 000 dinars
Intentionally disseminating personal data in a manner that harms the data subject or their privacy	Criminal	Imprisonment of 3 months and a fine of 3 000 dinars
Disseminating personal data in a manner that harms the data subject or their privacy without the intention of harm	Criminal	Imprisonment of 1 months and a fine of 1 000 dinars
Violation of the provisions requiring that data only be processed for the purposes for which it was collected, subject to some exceptions	Criminal	Imprisonment of 3 months and a fine of 1 000 dinars
Violation of the provisions requiring adequate security precautions to be taken to protect data being processed, or failure by a responsible party to choose a sub-contractor that takes adequate precautions	Criminal	Imprisonment of 3 months and a fine of 1 000 dinars
Violation of the provisions for responsible parties to correct or delete incorrect data, and to inform the data subject within two months	Criminal	Imprisonment of 3 months and a fine of 1 000 dinars
Failure by parties implementing automated processing to implement the necessary technical means to allow the data subject to electronically send a request for correction or erasure of personal data	Criminal	Imprisonment of 3 months and a fine of 1 000 dinars

Failure to destroy data within the necessary time period	Criminal	Imprisonment of 3 months and a fine of 1 000 dinars
Processing for longer than necessary to achieve the purposes for which it was implemented	Criminal	Imprisonment of 3 months and a fine of 1 000 dinars
Failure to destroy video-surveillance recordings when it is no longer necessary for achieving the purposes for which it was implemented	Criminal	Imprisonment of 3 months and a fine of 1 000 dinars
Collecting personal data for illegitimate purposes or contrary to public order, or processing data that is incorrect, not updated, or not necessary for the processing activity	Criminal	Imprisonment of 3 months and a fine of 1 000 dinars
Receiving data and failing to respect the guarantees and measures that the Authority set	Administrative	Fine of 10 000 dinars
Hindering the work of the Authority by impeding their investigation, refusing to provide requested documents, communicating in bad faith or providing incorrect information	Administrative	Fine of 5 000 dinars
Violation by a responsible party, subcontractor, bankruptcy trustee or liquidator who violates the provisions of article 24 around the cessation of data processing	Administrative	Fine of 1 000 dinars
Violation of the provisions relating to notification of the Authority in the case of a dispute with a data subject around the correctness of data	Administrative	Fine of 1 000 dinars