DRAFT DATA PROTECTION AND PRIVACY

Policy and Strategy, 2019

Abstract

Institutional and legal framework for data protection and privacy that will give effect to Section 23 of the Constitution of The Republic of The Gambia and to express the commitment of the Government to ensure the protection of personal data and associated rights of individuals, and in particular the right to privacy

Ministry of Information and Communication Infrastructure, The Gambia

OUTLINE

1. Introduction

Developments in ICT combined with the growth in connectivity and of internet enabled services are leading to the more intensive and automated collection and use of richly detailed personal data, in greater volumes, by the private and public sectors. While these developments are accelerating economic and social development opportunities and benefits, they are also generating new risks for individuals (around the world) requiring national policies and strategies.

The Government of The Gambia recognises the increasingly important role personal data plays in the development of the economy and society at large and wishes to adopt measures to help protect personal data and associated fundamental rights and freedoms, and in particular the right to privacy, to ensure public trust in the use of personal data. This is consistent with the Constitution of The Republic of The Gambia 1997 (the 'Constitution'). Section 23 of the Constitution recognises and sets out the right to privacy and further states that "*no person shall be subject to interference with the privacy of his or her home, correspondence or communications save as is in accordance with law and is necessary in a democratic society*."

The Government of The Gambia is also signatory to international instruments that establish privacy as a universal fundamental human right, such as the Universal Declaration of Human Rights (1948), the Convention on the Rights of the Child (1989) and the African Charter on the Rights and Welfare of the Child (1990). The Government wishes to build on the right to privacy enshrined in the Constitution and the above international instruments, and also on the Economic Community of West African States (ECOWAS) 'Supplementary Act on Personal Data Protection' (2010), the African Union Malabo Convention on Cybersecurity and Data Protection 2014 and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and its amending protocol (CETS No. 223) that requires Member States to establish a legal framework of protection for personal data and an individual's privacy.

The Government of The Gambia is also party to other international instruments such as the African Charter on Human and Peoples Rights (1981), that, like other instruments to which The Gambia is a party, recognises the importance of other fundamental rights and freedoms that may be impacted by the use of personal data beyond the right to privacy, such as the right to freedom of expression, and the right to freedom of association and assembly. A key aim of this policy, therefore, is to meet The Gambia's obligations and commitment arising from being party to the above international instruments, and to protect the personal data and associated rights and freedoms of individuals, and in particular the fundamental right to privacy.

The Policy reflects international developments within Africa and beyond and the increasing recognition of the need to make concrete, the protection of personal data and privacy in law, reflecting also the modernised Convention for the protection of individuals with regard the processing of their personal data (Convention 108+).

2. Purpose of the Policy

2.1 The purpose of this policy is to lay the foundations of institutional and legal framework for data protection and privacy that will give effect to Section 23 of the Constitution of The Republic of The Gambia and to express the commitment of the Government of The Gambia to ensure the protection of personal data and associated rights of individuals, and in particular the right to privacy.

3. Objective

The objective of this national data protection and privacy policy is to:

3.1 inform the development of data protection and privacy law to safeguard personal data and the rights to data protection and privacy of individuals;

3.2 help establish appropriate institutional frameworks to ensure the effective implementation and oversight of a national data protection and privacy law;

3.3 to establish internationally recognised best practice in data protection and privacy law;

3.4 ensure appropriate safeguards for the processing of special categories of personal data to prevent adverse effects for individuals;

3.5 ensure additional protections with regards to the processing of personal data about children in accordance with Article 10 of the African Charter on the Rights and Welfare of the Child (1990) and possibly for other vulnerable groups of individuals;

3.6 establish a requirement for an independent and impartial National Supervisory Authority appropriately empowered to sufficiently oversee, monitor and enforce compliance and safeguarding of the data protection and privacy rights of individuals;

3. Scope

4.1 The Policy applies to the processing of personal data in the private and public sectors, whether by automated or non-automated means and irrespective of the nationality or place of residence of the data subject;

4.2 The Policy does not apply to the processing of personal data made for personal or household purposes;

4.3 The policy applies to personal data or special categories of data about living individuals. The policy does not apply to data about deceased persons;

4.4 The policy applies to data processing undertaken within the jurisdiction of The Gambia.

4. Basic Principles for the Protection of Personal Data

The Principles outlined in this section are based on international best practice taking into consideration the Malabo Convention and the modernised and most widely adopted globally, Convention 108+.

As a prerequisite, the policy requires that personal data and special categories of data are processed fairly, lawfully and transparently and in a manner that is proportionate in relation to the legitimate purpose(s) pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms of individuals at stake.

5.1 Fair, transparent and lawful processing

5.1.1 Personal data shall be processed **fairly**

5.1.2 Personal data must be processed in a **transparent** manner. Data subjects have right to know about the processing of their personal data. Controllers should be required to act transparently to ensure fairness of processing and to inform data subjects in an appropriate form of the controller's identity and other key information about the processing and their rights in order to ensure fair and legitimate processing.

5.1.3 Personal data must be processed **lawfully** and have a legitimate basis as set out in Section 6.

5.2 Specific Legitimate Purpose and Purpose Limitation

5.2.1 Personal data must be processed for explicit, specified and legitimate purposes and the processing of that particular data must serve those purposes and shall not be incompatible with them.

5.2.2 Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes may be considered compatible with those purposes, subject to appropriate safeguards.

5.3 Data Minimisation

5.3.1 Personal data undergoing processing should be adequate, relevant and not excessive in relation to the purposes for which they are processed.

5.3.2 This requirement not only refers to the quantity, but also to the quality of personal data.

5.4 Accuracy

5.4.1 Personal data undergoing processing should be accurate and, where necessary, kept up to date.

5.5 Storage Limitation

5.5.1 Personal data undergoing processing should be preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.

5.5.2 Personal data should be deleted once the purpose for which it was processed has been achieved, or that it should only be kept in a form that prevents any direct or indirect identification of the data subject.

5.6 Data Security and Security Breach Notification

5.6.1 The controller, and, where applicable the processor, shall take appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data.

5.6.2 The controller shall notify, without delay, at least the competent supervisory authority of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.

5.7 Accountability

5.7.1 Controllers (and, where applicable, processors), shall take all appropriate measures to comply with the provisions set out in this policy and applicable data protection and privacy law, and be able to demonstrate that the data processing under their control complies with them.

6. Legitimate Basis

The processing of personal data must be carried on at least one of the legitimate bases in this section, and for a specified and legitimate purpose:

6.1 based on the data subject's consent. Such consent that must be freely given, specific, informed and unambiguous, or;

6.2 necessary for the fulfilment of a contract with the data subject, or;

6.3 necessary to protect the vital interests of the data subject or of another person, or;

6.4 necessary for compliance with a legal obligation, or;

6.5 carried out on the basis of grounds of public interest, or;

6.6 for overriding legitimate interests of the controller or of a third party

7. Special Categories of Data

The processing of certain types of data, or the processing of certain data for the sensitive information it reveals, may lead to encroachments on the interests, rights and freedoms of individuals. This can for instance be the case where there is a potential risk of discrimination or injury to an individual's dignity or physical integrity, where the data subject's most intimate sphere, is being affected, or where processing of data could affect the presumption of innocence or other important rights and freedoms.

7.1 The processing of the following categories of data shall only be allowed where appropriate safeguards that are complementing those that are enshrined in the data protection and privacy law:

(a) genetic data;
(b) personal data relating to offences, criminal proceedings and convictions, and related security measures;
(c) biometric data uniquely identifying a person;
(d) personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life.

7.2 The safeguards shall guard against risks that the processing of such data may present for the interests, rights and freedoms of the data subject, notably the risk of discrimination.

7.3 Appropriate safeguards include, where the processing is carried out:

(a) with the data subject's explicit consent;

(b) under a professional secrecy obligation;

(c) a law covering the intended purpose and means of the processing or indicating the exceptional cases where processing such data would be permitted;

(d) a particular and qualified organisation;

(e) processing is necessary to protect the vital interests of the data subject or of another natural person.

8. Data Protection and Privacy by Design and Default

8.1 Before carrying out processing, controllers (and, where applicable, processors), shall examine its potential impact on the rights and fundamental freedoms of data subjects prior to the commencement of the processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.

8.2 Controllers (and, where applicable, processors), shall implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.

8.2 This implementation of data protection requirements should be achieved not only as regards the technology used for processing the data, but also the related work and management policies and processes.

8.3 When setting up the technical requirements for default settings, controllers and processors should choose privacy-friendly standard configurations so that the usage of applications and software does not infringe the rights of the data subjects (data protection by default), and to avoid processing more data than necessary to achieve the legitimate purpose.

9. Transborder Flows of Personal Data

The free flow of data is essential to the expansion of the digital economy, to harness all the benefit of digitisation and new data processing techniques and technologies can bring to society and that can contribute greatly to the inclusive growth of a country. However, it is essential to ensure that at least the same level of protection is afforded to personal data when transferring them across borders that is foreseen and guaranteed within the jurisdiction of The Gambia. The cross-border transfer of personal data therefore may only take place where an appropriate level of protection is guaranteed.

9.1 An appropriate level of protection can, after a thorough assessment by the data controller, be secured by:

(a) the law of the receiving country or international organisation, including the applicable international treaties or agreements, or;

(b) ad hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing

9.2 Notwithstanding the provisions of the previous paragraphs the transfer of personal data may also take place if:

(a) the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards;

(b) the specific interests of the data subject require it in the particular case;

(c) in response to prevailing legitimate interest, in particular an important public interest, if it is provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society;

(d) it constitutes a necessary and proportionate measure in a democratic society for the freedom of expression.

9.3 The supervisory authority is preferably to be involved in assessing if the criteria are met when using the above-mentioned exceptions.

9.4 The supervisory authority is entitled to request that the data controller which transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests.

9.5 The supervisory authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit such transfers, suspend them or subject them to condition.

9.6 For international law enforcement co-operation the same requirements should be applicable and proper legal bases for the transfer should be established and ensured. For this latter, joining international treaties (such as the Africa Union Malabo and Council of Europe Budapest Conventions), using appropriate international frameworks (as guaranteed by Interpol instruments) which enable the international cooperation in specific investigations related to

specific crimes while alone or with other instruments guaranteeing the appropriate level of protection during the transfer between participating states could be envisaged.

10. Rights of Data Subjects

10.1 Every individual shall have a right:

(a) not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration;

(b) to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing

(c) to obtain, on request, knowledge of the reasoning underlying the processing of personal data about them;

(d) to object at any time to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms;

(e) to obtain, on request, free of charge and without excessive delay, the rectification or erasure of such data processed contrary to the provisions of this policy and the proposed law;

(f) to obtain, on request, free of charge and without excessive delay judicial and non-judicial remedy for violations of the law;

(g) to benefit, whatever his or her nationality or residence, from the assistance of the Supervisory Authority in exercising his or her rights

10.2 Paragraph 1(a) shall not apply if the decision is authorised by a law to which the controller is subject, and which also

lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

11. Exceptions

11.1 The right to privacy and personal data are not absolute rights. They have to be balanced with other human rights (with the exception of the right to life and to human dignity) and may be subject to specific exceptions for the lawful processing of personal data undertaken for important public or private interests.

11.2 The use of exceptions and restrictions must be subject to objective legal requirements to be considered lawful and to guard against their arbitrary application. According to objective criteria all exceptions or restrictions have to be provided for by law, pursue a legitimate purpose, respect the essence of the fundamental rights and freedoms and constitute a *necessary* and *proportionate* measure in a democratic society.

11.3 No blanket or unnecessarily broad exceptions should be defined in the law and there should not be entire sectors or activities exempted from the scope or the application of all provisions of the law. Processing activities for national security and defence purposes shall be subject to independent and effective review and supervision.

12. Establishment of a Supervisory Authority

12.1 A key objective of this policy is to identify an independent and impartial National Supervisory Authority ('Supervisory Authority') appropriately empowered to oversee, monitor and enforce compliance and safeguarding of the data protection and privacy rights of individuals.

12.2 Under this policy, the Supervisory Authority shall be empowered by a Data Protection Act (The Act) as an independent administrative body. The Act shall ensure that the authority is empowered as a statutory independent and impartial Authority, the scope of its mandate, it's powers, ability to acquire a property, sue and be sued.

12.3 Consistent with the Government of The Gambia's recognition of the right to privacy as a fundamental human right (by virtue of Section 23 of the Constitution and by

being party to international human rights conventions), The Act should expressly confirm that the authority will treat the privacy of an individual as a fundamental human right.

12.4 The authority is usually the institution mandated by The Act to protect the rights of the individuals, their personal data, determine the process by which it is processed and compliance with the provisions of the African Union Malabo Convention and Council of Europe Convention 108+ such as:

(a) have powers of investigation and intervention;

(b) perform the function of authorising and approving standardised safeguards relating to transborder data flows;

(c) make determinations relating to violations of the Act and impose the necessary administrative sanctions;

(d) instigate legal proceedings;

(e) issue or otherwise issue opinions and approve statuary Codes of Conduct or Guidelines relating to the processing of personal data;

(f) publishing reports of their activities.

12.5 The authority's mandate should include the responsibility to take part in international cooperation, to promote public awareness of their functions, powers and activities; the rights of data subject and exercise of such rights; and awareness of controllers, processors and their legal obligations under the Act especially in processing special category data such as that of children and other vulnerable individuals.

12.6 The authority shall be consulted on proposals for any legislative or administrative measures involving the processing of personal data, and requests and complaints from data subjects

12.7 Staff of the authority

The authority should be provided with the necessary resources to enable it to appoint skilled staff and or build internal capacity to enable the effective performance of its functions. Staff of the authority may be bound by the obligations of confidentiality in the performance of their duties and exercise of powers.

The authority may appoint specialist staff or consultants to enable it to deliver its mandate.

12.8 International Cooperation

The Act may empower the Authority to perform the data protection functions that are necessary to give effect to any international obligations such as required by the Convention 108+ and the Malabo Convention, including assistance to data subjects.

13. Strategies and Action Plan

The present Action plan summarises the most important and relevant actions to be taken by the government to give effect to the determination of The Gambian government to ensure the protection of individual's privacy and personal data in the digital age that are compliant with international standards and to implement the Privacy and Data Protection Policy of The Gambia. These actions can be complemented by other already existing and future actions laid down in the government strategic plans.

13.1 Adoption of the national legislation

I. to draft a modern and robust Bill for the Protection of privacy and personal data in The Gambia
II. to ensure that the Bill is aligned to international standards by seeking the assistance from international organisations, such as the Council of Europe in the drafting
III. to conduct public consultation on the draft Bill, to incorporate the outcome
IV. to ensure the consultation of all relevant public institution, to incorporate the outcome
V. to ensure that the draft Bill is compliant with other national legislation, international commitments, to propose amendment of existing legislation, if required
VI. to raise awareness on the draft bill by targeted public relations and media campaigns, events (possibly in cooperation with international partners, such as ECOWAS, African Union and the Council of Europe) on, but not exclusively, the international Data Protection Day (28 January), to produce information leaflets and to distribute among the population and ensure their online publication
VII. to present the draft Bill to the National Assembly

13.2 Establishment of the Gambian Data Protection Authority

I. to identify an authority to shoulder the Data Protection and Privacy mandate for the Protection of privacy and personal data in The Gambia
II. to prepare and to present the new chapter on the Gambian Data Protection authority in the state budget according to the Law on the Protection of privacy and personal data in The Gambia, to prepare the estimation of the funds and resources necessary for the functioning of the Gambian Data Protection authority;
III. to seek possibilities for assistance in the establishment and the funding of the Gambian Data Protection authority from available development programs led by international organisations such as ECOWAS, African Union and the Council of Europe;
IV. to ensure the capacity building and the training of the future staff of the Gambian Data Protection authority (also possibly in cooperation with international organisations)
V. to raise awareness on the Gambian Data Protection Authority within the national administration, in the country in general and until its establishment, internationally too.

13.3 Creation of an Industry Data Protection and Privacy Professionals

It is important to have a pool / industry of professionals and to ensure continuous capacity building in the subject matter to serve data controllers and processors operating in The Gambia.

This can be achieved through taking the following measures:

- conducting a capacity gap assessment on data protection and privacy in the country, through collaboration with international partners.
- Training of trainers
- Introduction of certificate and diploma programs which could be certified by the Data Protection Authority and this can be a source of funding for authority.

13.4 Sensitisation and awareness raising

Sensitisation is a key component towards the achievement of the goals of this policy. This could be achieved through using media and also annually celebrating the globally set aside Privacy Day, i.e. 28 January.

14. Definitions

For the purposes of this policy:

(a) "personal data" means any information relating to an identified or identifiable individual ("data subject");

(b) "data processing" means any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data;

(c) Where automated processing is not used, "data processing" means 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;

(d) "controller" means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making power with respect to data processing;

(e) "recipient" means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;

(f) "processor" means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.