DATA PROTECTION AND PRIVACY BILL, 2024

DATA PROTECTION AND PRIVACY BILL OF THE GAMBIA, 2024

ARRANGEMENT OF SECTIONS

Section

DATA PROTECTION AND PRIVACY BILL, 2024

DATA PROTECTION AND PRIVACY BILL, 2024

A BILL ENTITLED

AN ACT to regulate the processing of personal data in order to promote and protect the human rights and fundamental freedoms of individuals and, in particular, the right to privacy, and for connected matters.

[ ]

ENACTED by the President and the National Assembly.

PART I – PRELIMINARY

1. Short title

This Bill may be cited as the Personal Data Protection and Privacy Bill, 2024.

2. Interpretation

In this Act –

"anonymisation" means the process applied to personal data so that the data subjects can no longer be identified, either directly or indirectly;

"anonymous data" means information which does not relate to an identified or identifiable data subject or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable and from which it is impossible to re-identify the data subject taking into consideration the available technology at the time of the processing and technological developments;

"automated individual decision-making and profiling" means a decision based solely on automated processing and profiling;

"biometric data" means personal data relating to the physical, biological, physiological or behavioural characteristics which permit the unique identification or authentication of an individual, including by facial images or dactyloscopy biometric or fingerprint data;

"child" means a person who is under the age of eighteen years;

[Cap. 45:01]

"Commission" means the Information Commission established under the Access to Information Act;

[Act No. 10 of 2021]

"consent" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the specified processing of personal data relating to him or her;

"Controller" means –

(a) the natural or legal person, public authority, service, agency or a body which, alone or jointly with others, has decision-making powers determining the purposes and means of the processing of personal data; or

(b) a natural person, legal person or public body that has been designated as such by that act, decree or ordinance.

"data protection officer" means a person designated by the data controller or a processor;

"data subject" means an identified or identifiable living individual to whom personal data relates;

"direct marketing" means the communication of any advertising or marketing material which is directed to any particular individual;

"genetic data" means any personal data relating to the genetic characteristics of an individual which have been either inherited or acquired during prenatal development, as they result from an analysis of a biological sample from the individual concerned, in particular chromosomal, Deoxyribonucleic acid (DNA) or Ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained;

"Identified or Identifiable individual" means a person who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity;

"information society services" means services provided for remuneration, at a distance, with electronic means and on individual request of the recipient of the service and include, in particular, the sale of goods and services, services of access to information or advertising over the internet and access to public communications network services, transmission of data, or storing the recipient's data in the public communications network;

"international organisation" means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

"joint data controllers" means two or more controllers, that jointly have decision-making power with respect to data processing;

"personal data" means any information relating to an identified or identifiable individual;

"personal data breach" means a breach of security leading to the accidental or unlawful use, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"processing" means any operation or set of operations performed on personal data whether or not it occurs by automatic means, such as the collection, recording, storage, preservation, access, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical or arithmetical operations on such data;

"processor" means a natural or legal person, public authority, service, agency, or any other body which is authorised to processes personal data on behalf of the controller. Instructions that a controller is required to provide to a processor shall limit what the processor is permitted to do with the personal data;

"profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular, to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

"pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information that is kept separately and subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual;

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

"restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future;

"special categories of personal data" means genetic data; biometric data; personal data relating to offences, criminal proceedings and convictions; personal data revealing racial or ethnic origin, political opinions, trade-union membership, religious beliefs, health or data concerning an individual's gender. The processing

of such data shall be prohibited or allowed only subject to appropriate safeguards under section 6; and

"third-party" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

3. Application

(1) This Act applies to the processing of personal data –

(a) wholly or partly, by automated means and non-automated means where the personal data forms part of a structured set of data and are accessible or retrievable according to specific criteria and which allows the search, combination or attribution of data to a specific data subject;

(b) carried out by controllers, and where applicable processors established in the territory of The Gambia; and

(c) undertaken outside the territory of The Gambia where the processing relates to individuals within the jurisdiction of The Gambia.

(2) This Act does not apply to –

(a) data processing carried out by an individual in the course of purely personal or household activities; and

(b) anonymous data.

PART II – BASIC PRINCIPLES AND LAWFUL PROCESSING

4. Principles relating to the processing of personal data

(1) A controller must ensure that personal data is processed –

(a) fairly, transparently and lawfully; and

(b) for explicit, specified and legitimate purposes consistent with the provisions of this Act.

(2) A data subject must be informed by the controller of his or her right to know about the processing of his or her personal data in accordance with this Act.

(3) In determining whether further processing of personal data is compatible with the original purpose, the controller must assess –

(a) The relationship between the original purpose and the purpose of the further processing;

(b) The purpose of the further processing;

(c) The context in which the personal data was collected, including the data subject's reasonable expectations based on their relationship with the controller regarding future use;

(d) The nature of the personal data;

(e) The potential impact of the further processing on a data subject; and

(f) The existence of appropriate safeguards in both the original processing and the further processing.

(3) The processing of personal data for archiving in the public interest, scientific or historical research, or statistical purposes by a controller is permitted, subject to the provisions of this act on the preservation of personal data.

(4) A controller must ensure that personal data undergoing processing is –

(a) adequate, relevant and not excessive in relation to the purpose for which they are processed; and

(b) accurate and, to the extent necessary, be kept up to date.

(5) A controller must take reasonable steps to ensure that personal data that is inaccurate is rectified or erased without delay.

(7) A controller may store personal data for longer periods insofar as it will be processed solely in the public interest for archiving, scientific or historical research purposes subject to applicable laws on the preservation of personal data.

(8) A controller must ensure that personal data is erased once the purpose for which it was processed has been achieved or where it is stored for longer periods subject to subsection (7), shall only be kept in a form that prevents any direct or indirect identification of the data subject.

(9) A controller must process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures, in accordance with this Act.

(10) A controller must process personal date in a manner that safeguards against adverse consequences for individuals. The choice of the technology ensuring the best available security of data is left with the data controller taking into account the context of the intended data processing.

(11) A controller must be responsible for, and be able to demonstrate compliance with the provisions under this section.

5. Lawful processing of personal data

(1) A controller must ensure that the processing of personal data is proportionate to the purpose pursued, taking into account the interests, rights and freedoms of data subjects.

(2) The processing of personal data by a controller is considered lawful if –

(a) the data subject has given consent to the processing of his or her personal data for one or more specified purposes subject to the conditions of consent set out in this Act;

(b) it is for the purpose of entering into or the performance of a contract to which the data subject is a party;

(c) it is for compliance with a legal obligation to which the controller is subject;

(d) it is necessary in order to protect the vital interests of a data subject or of another person;

(e) it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) it is necessary for the purpose of the legitimate interest of the controller or by a third-party to the extent that such an interest does not override the interest or fundamental rights and freedoms of a data subject; or

(g) it is carried out for archiving purposes in the public interest, or for scientific or historical research purposes or statistical purposes, subject to appropriate safeguards for the rights and freedoms of data subjects.

(3) subsection (2) (f) does not apply to the processing of personal data by a public authority in the performance of his or her duty under any other law.

(4) Where the processing is carried out for a purpose which is not the original purpose for which the personal data were collected, a controller shall carry out an assessment and take into account –

(a) the context in which the personal data were originally collected and the compatibility of the new purpose, and the reasonable expectations of the data subjects;

(b) any link between the original purpose for which the personal data were collected and the intended additional processing of the personal data;

(c) the nature of the personal data to be processed, including any additional protections afforded, such as for special categories of personal data or data related to criminal offences and convictions; and

(d) any possible consequences for data subjects, including any prejudice or harm to their rights and freedoms.

6. Processing of special categories of personal data

(1) A Controller shall ensure that the processing of special categories of data proceeds only where additional appropriate safeguards for the protection of the fundamental rights and interests of the data subject are in place and at least one of the following applies –

(a) the processing is provided for by law or the data subject has given explicit consent to the processing of his or her personal data for one or more specific purposes subject to the conditions of consent set under this Act;

(b) the processing is necessary to –

(i) assess the capacity of an employee,
(ii) carry out the obligations and exercising specific rights of the controller,
(iii) exercise specific rights of the data subject in a field of employment, or
(iv) manage the social security system and services, subject to conditions provided for by law;

(c) The processing is necessary in the management of health services or pursuant to a contract with a health professional, subject to professional secrecy and conditions provided for by law;

(d) processing is necessary for monitoring and protecting against a life-threatening epidemic and its spread or for the purpose of humanitarian actions, subject to specific measures to safeguard the rights and freedoms of data subjects provided for by law;

(e) processing is necessary to protect the vital interests of the data subject or of another individual where the data subject is physically or legally incapable of giving consent;

(f) processing is necessary for the protection of national security, defence, public safety, and prosecution of criminal offences, subject to specific measures to safeguard the rights and freedoms of data subjects provided for by law;

(g) processing is carried out in the course of its legitimate activities by a non-profit body and on condition that the processing relates solely to the members or to persons connected to its purposes and that the personal

data are not disclosed outside that body without the consent of the data subjects;

(h) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or

(i) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions provided for by law.

7. Processing personal data of a child

(1) Where a controller processes the personal data of a child, he or she shall ensure that the child's -

(a) privacy is fully respected, and

(b) best interest is given primary consideration.

(2) A controller shall apply specific safeguards to –

(a) the use of personal data of a child for the purpose of marketing or profiling; and

(b) the collection of personal data of a child that makes use of a service offered directly to children.

(3) Where a controller is processing of the child's personal data, he or she must ensure that the information about the processing is in a clear and plain language that the child can easily understand.

(4) A child's consent shall not be deemed valid where processing of the child's data creates a risk to or infringes the best interests of the child.

(5) Processing of personal data under this section is lawful where –

(a) it is based on the consent given by the child's parent, guardian, or legal representative;

(b) it is in the interests of the child as determined by his or her parent, guardian, or legal representative;

(c) it is necessary to meet a legal obligation to which the controller is subject;

(d) it is necessary for the performance of a task carried out by the controller in the interest of the public in accordance with the law; or

(e) it is necessary in the context of preventive or counselling services offered directly to a child.

8. Conditions for Consent

(1) Where the processing of personal data is based on consent, the controller must provide evidence of the data subject's consent.

(2) Consent must be obtained freely, either electronically, in writing, or through an oral statement that clearly indicates the data subject's acceptance of the processing.

(3) Requests for consent must be clearly distinguishable from other matters, using clear and plain language that is easily understood.

(4) Consent must cover all processing activities related to the same purpose and where there are multiple purposes, consent must be obtained for each specific purpose.

(5) A data subject may withdraw consent at any time before, during, or after the processing.

(6) Before obtaining consent, the data subject must be informed of their right to withdraw consent and the process for doing so.

(7) The withdrawal of consent does not affect the lawfulness of processing carried out before the controller received the withdrawal.

(8) Where the controller continues processing after receiving a withdrawal of consent, the processing is deemed unlawful unless the controller proves that it is based on a lawful basis under this Act.

(9) Consent is not considered freely given if the data subject cannot refuse or withdraw consent without suffering any disadvantage or undue influence.

PART III - RIGHTS OF THE DATA SUBJECT

9. Right to know and access

(1) A Data subject has the right to obtain, on request and at reasonable intervals, confirmation of whether his or her personal data is being processed and where data is being processed, the data subject is entitled to receive the following information -

(a) The purposes of the processing;

(b) The source of the personal data being processed;

(c) The recipients or categories of recipients to whom the personal data is disclosed;

(d) Where applicable, the controller's intention to transfer personal data to a country or international organisation outside The Gambia;

(e) Any other information the controller is required to provide to ensure transparency of processing, as per section 25;

(f) The period for which the personal data will be retained;

(g) The reasoning behind the processing where its results are applied to the data subject, including any consequences of such reasoning; and

(h) A copy of the personal data being processed.

(2) Where personal data is being processed, the controller must provide a copy of the data free of charge and in an intelligible form, along with the information specified in subsection (1), without undue delay and no later than one month after receiving the request.

(3) The one-month period may be extended by an additional month if necessary, considering the complexity of the request and in responding.

(4) A controller must provide reasons for any delay in responding to a request under this section.

(5) In exceptional cases, where a request under subsection (2) is manifestly excessive or unfounded, particularly due to its repetitive nature, the controller may –

(a) charge a reasonable fee based on administrative costs incurred; or
(b) refuse to act on the request.

(6) Where a controller charges a fee under subsection (5)(a) or refuses a request under subsection (5)(b), the controller bears the burden of proving that the request is manifestly excessive or repetitive.

(6) Limits on fees for the purpose of subsection 5 (a) shall be provided for by law.

10. Right to rectification, erasure, and restriction of processing

(1) A data subject has the right to obtain, without undue delay and free of charge, the rectification of inaccurate or incomplete personal data from the controller which may include the recording of a supplementary statement.

(2) A data subject has the right to obtain, without undue delay and free of charge, the erasure of personal data where –

(a) the data is no longer necessary for the purpose for which it was collected or processed;

(b) the data subject withdraws consent and no other lawful basis exists for processing the data;

(c) the data subject objects to the processing, and the controller cannot demonstrate overriding lawful grounds in accordance with this Act;

(d) the personal data is being processed unlawfully; or

(e) the personal data must be erased to comply with a legal obligation to which the controller is subject.

(3) A data subject has the right to obtain the restriction of personal data processing, for a necessary period, where –

(a) the accuracy of the personal data is contested by the data subject;

(b) the controller no longer requires the personal data, but the data subject needs it for the establishment, exercise, or defense of a legal claim; or

(c) the data subject objects to the processing of personal data based on section 6(1)(e) or (f) of this Act, pending justification from the controller that their lawful interests override those of the data subject.

(4) Where a data subject has submitted a valid request for rectification, erasure, or restriction of personal data under subsections (1), (2), or (3), the controller must communicate the request to all recipients of the personal data.

(5) Complete rectification, erasure, or restriction must be carried out in accordance with subsection (2), unless the controller can demonstrate that doing so would be impossible or require disproportionate effort.

11. Right to object

(1) A data subject has the right, at any time and free of charge, to object to the processing of their personal data based on their specific situation unless the controller can demonstrate lawful grounds that override -

(a) the data subject's interests;

(b) the data subject's fundamental rights and freedoms; or

(c) the establishment, exercise, or defense of a legal claim.

(2) A data subject has the right, at any time and free of charge, to object to the processing of their personal data for direct marketing purposes, including profiling related to such marketing

(3) Where a data subject objects to the processing of their personal data for direct marketing, the controller must cease processing the data for that purpose.

(4) Unless as provided in subsection (2), personal data processed for direct marketing via electronic means requires the prior consent of the data subject, in accordance with section 8.

(5) A controller may send direct marketing communications by electronic means without prior consent if the controller has obtained the data subject's electronic contact details during the sale or negotiation of a product or service, provided that –

(a) the marketing relates only to the controller's own similar products or services;

(b) the data subject is clearly informed, in plain language, of the intention to send marketing communications and the means by which they will be sent; and

(c) the data subject is given the opportunity to refuse direct marketing both at the time of collection of their contact details and in each subsequent communication.

12. Right not to be subject to automated decision making

(1) A data subject has the right not to be subject to a decision that significantly affects him or her, based solely on automated processing of his or her personal data, without his or her views being taken into account.

(2) Subsection (1) does not apply if the decision –

(a) is authorised by law applicable to the controller, which includes appropriate measures to safeguard the legitimate interests, rights, and freedoms of data subjects;

(b) is necessary for entering into or performing a contract between the data subject and the controller; or

(c) is based on the data subject's consent, provided that appropriate safeguards are in place.

(3) Where subsection (2)(a) or (2)(c) applies, the controller must implement suitable measures to safeguard the data subject's rights, freedoms, and legitimate interests.

(4) Where a decision under subsection (2) is based on special categories of personal data as defined in section 6(1), the processing can only proceed if the conditions set out in sections 28 and 31 are met and the processing is authorised by law and necessary for reasons of substantial public interest.

13. Right to obtain assistance from the Commission

A data subject has the right to seek assistance from the Commission in exercising his or her rights under this Act.

14. Representation of the data subject

(1) A data subject has the right to authorise a not-for-profit body, organisation, or association that is properly constituted under the laws of The Gambia and active in the protection of fundamental rights and freedoms to -

(a) lodge a complaint with the Commission on behalf of the data subject;

(b) pursue a judicial remedy on behalf of the data subject against a legally binding decision of the Commission; or

(c) pursue a judicial remedy on behalf of the data subject against a data controller or processor.

(2) An organisation referred to in subsection (1) has the right to lodge a complaint with the Commission if it believes the rights of data subjects under this Act are being systematically infringed or if the issue affects the rights and freedoms of a large number of individuals.

15. Right to remedy

(1) A data subject has the right to seek a remedy, including judicial remedy, in accordance with the laws of The Gambia.

(2) The intervention of the Commission does not prevent a data subject from seeking a judicial remedy.

(3) A data subject who suffers material or non-material damage as a result of an infringement of this Act has the right to compensation from the controller or processor, in accordance with the laws of The Gambia.

(4) A controller involved in processing is liable for any damage caused by processing that infringes the provisions of this Act.

(5) A processor is liable for damage caused by processing if it has failed to comply with obligations specifically directed at processors or if it acted outside or contrary to the lawful instructions of the controller.

(6) A controller or processor is exempt from liability under subsection (3) if it can prove that it is not responsible for the event that caused the damage.

PART IV – OFFENCES

16. Unlawful processing of personal data

(1) A person who knowingly or recklessly obtains, retains, discloses, or procures the disclosure of personal data without the controller's authorisation, with the intent of financial gain or to cause harm to specific data subjects, commits an offence and is liable on conviction to -

(a) in the case of an individual, a fine not exceeding one million dalasis, imprisonment for a term not exceeding three years, or both; and

(b) in the case of a body corporate, a fine of not less than five million dalasis.

(2) It is a defence for a person charged under subsection (1) to prove that the obtaining, disclosure, procuring, or retaining of the personal data –

(a) was required or authorised by law or by a competent judicial authority; or

(b) was justified in the public interest or necessary and proportionate for the investigation and prosecution of a specific criminal offence.

(3) It is also a defence for a person charged under subsection (1) to prove that they reasonably believed that –

(a) they had a legal basis to obtain, retain, disclose, or procure the personal data; or

(b) the controller would have authorised the obtaining, retaining, disclosure, or procuring of the personal data.

17. Selling personal data

(1) A person who sells or offers to sell personal data, or advertises that personal data is or may be for sale, commits an offence and is liable on conviction –

(a) in the case of an individual, to a fine not exceeding two million dalasis, imprisonment for a term not exceeding ten years, or both; and
(b) in the case of a body corporate, to a fine not exceeding ten million dalasis.

(2) A person who sells or offers to sell personal data, or advertises that personal data is or may be for sale, where the data was obtained in circumstances involving an offence under section 16 (1), commits an offence and is liable on conviction –

(a) in the case of an individual, a fine not exceeding five million dalasis, imprisonment for a term not exceeding ten years, or both; and

(b) in the case of a body corporate, to a fine of not less than ten million dalasis.

18. Impersonating or falsely pretending to be a data subject

(1) A person who misleads the Commission, a controller, or, where applicable, a processor by impersonating a data subject, falsely pretending to be a data subject, or falsely claiming to act under the authority of a data subject for the purpose of -

(a) obtaining access to that data subject's personal data; or

(b) having that data subject's personal data used, altered, or destroyed,

commits an offence.

(2) A person who commits an offence under subsection (1) is liable on conviction –

(a) in the case of an individual, to a fine not exceeding two million dalasis, imprisonment for a term not exceeding seven years, or both; and

(b) in the case of a body corporate, to a fine not exceeding ten million dalasis.

19. Re-identification of personal data

(1) A person who knowingly or recklessly re-identifies personal data without the authorisation of the controller responsible for anonymizing the data commits an offence and is liable on conviction to –

(a) in the case of an individual, to a fine not exceeding one million dalasis, imprisonment for a term not exceeding three years, or both; and

(b) in the case of a body corporate, to a fine not less than one million dalasis.

(2) For the purposes of this section, a person "re-identifies" information if they take steps that result in the information no longer being anonymised, as defined under section 2.

(3) It is a defence for a person charged under subsection (1) to prove that the re-identification –

(a) was required or authorised by law or by a competent judicial authority;
(b) was justified in the public interest; or

(c) was a necessary and proportionate measure for the investigation and prosecution of a specific criminal offence.

(4) It is also a defence for a person charged under subsection (1) to prove that they acted in the reasonable belief that –

(a) they are the data subject to whom the information relates;

(b) they had the consent of the data subject; or

(c) they had the authorisation of the controller.

20. Alteration of personal data to prevent disclosure to a data subject

(1) A person who alters, erases, destroys, or conceals all or part of personal data with the intent to prevent its disclosure to a data subject entitled to access under section 9 commits an offence.

(2) A person who commits an offence under subsection (1) is liable on conviction –

(a) in the case of an individual, to a fine not exceeding one million dalasis, imprisonment for a term not exceeding three years, or both; and

(b) in the case of a body corporate, to a fine not exceeding five million dalasis.

(3) It is a defence for a person charged under subsection (1) to prove that the alteration, erasure, destruction, or concealment of personal data was –

(a) required or authorised by law or by a competent judicial authority;

(b) justified in the public interest; or

(c) a necessary and proportionate measure for the investigation and prosecution of a specific criminal offence.

21. Concealment of a personal data security breach

(1) A person who conceals a personal data security breach with the intention of preventing disclosure of information to the Commission and where applicable, a data subject, commits an offence.

(2) A person who commits an offence under subsection (1) is liable on conviction –

(a) in the case of an individual, to fine of not more than one million dalasis or imprisonment for a term not more than two years or to both fine and imprisonment; and

(b) in the case of a body corporate, to a fine of not more than three million dalasis.

(3) It is a defence for a person charged with an offence under subsection 1 to prove that concealment of a personal data security breach –

(a) was required or authorised by law or by a competent judicial authority; or

(b) was justified in the public interest or was a necessary and proportionate measure for the investigation and prosecution of a specific criminal offence

22. False statements made in response to a notice requesting information

(1) A person who, in response to a notice from the Commission requesting information, makes a false or misleading statement or knowingly provides false or misleading information commits an offence.

(2) A person who commits an offence under subsection (1) is liable on conviction –

(a) in the case of an individual, to a fine not exceeding one million dalasis, imprisonment for a term not exceeding seven years, or both; and

(b) in the case of a body corporate, a fine not exceeding ten million dalasis.

23. Destruction or falsification of information requested by the Commission

(1) A person who destroys, conceals, or falsifies any information, document, equipment, or material with the intent to prevent its disclosure to the Commission during its exercise of investigative powers commits an offence.

(2) A person who obstructs, hinders, or resists the Commission while it exercises its investigative powers, or fails to comply with any lawful requirement of the Commission, commits an offence.

(3) A person who commits an offence under this section is liable on conviction –

(a) in the case of an individual, to a fine not exceeding one million dalasis, imprisonment for a term not exceeding seven years, or both; and

(b) in the case of a body corporate, to a fine not exceeding ten million dalasis.

24. Criminal liability of a body corporate

(1) An offence committed by a body corporate is deemed to be committed by any person who, at the time of the offence, is -

(a) a director, general manager, secretary, or similar officer of the body corporate; or

(b) acting or purporting to act in such a capacity.

(2) Sub-section (1) does not apply to a person if –

(a) the offence was committed without their consent or knowledge; and

(b) the person exercised all due diligence to prevent the offence, considering the nature of their functions and the surrounding circumstances.

PART V – OBLIGATIONS OF CONTROLLERS AND PROCESSORS

25. Transparency

(1) Controllers must act transparently to ensure fair processing of personal data and must inform data subjects in an appropriate manner about the information specified in subsection (2), as well as their rights under Part III.

(2) When obtaining personal data, either directly or indirectly, controllers must provide the data subject with the following minimum information, in a clear and accessible manner –

(a) the controller's identity and the contact details of his or her habitual residence;

(b) the legal basis and the purposes of the intended processing;

(c) the categories of personal data processed;

(d) the recipients or categories of recipients of the personal data, if any; and

(e) the means of exercising the rights set out in Part III.

(3) Subsection (2) does not apply where the data subject already has the relevant information.

(4) Where personal data is not collected directly from the data subject, controllers are not required to provide the information under subsection (2) if –

(a) the processing is prescribed by law; or
(b) providing the information is impossible or would involve disproportionate effort after an assessment.

(5) Where a controller relies on subsection (4)(b), he or she must demonstrate, on a case-by-case basis, the factors that led to the conclusion that providing the

information under subsection (2) is impossible or would involve disproportionate effort.

26. Joint controllers

(1) Joint controllers must determine their respective responsibilities and roles to ensure compliance with their obligations under this Act, particularly concerning the exercise of data subject rights and the cross-border transfer of personal data.

(2) The distribution of responsibilities between joint controllers must be made available to the data subject.

(3) The data subject may freely exercise their rights in relation to and against any of the joint controllers, as provided under this Act.

27. Processor

(1) Where processing is carried out on behalf of a controller, the controller must only use processors that provide sufficient guarantees to implement appropriate technical and organisational measures to ensure compliance with this Act and protect the rights and freedoms of individuals.

(2) Processing by a processor must be governed by a contract or by law, which specifies the subject matter, duration, nature, and purpose of the processing, the type of personal data and categories of data subjects, as well as the obligations and rights of the controller.

(3) A processor must not engage another processor without the prior written authorisation of the controller.

(4) Where a processor engages another processor to perform specific processing activities, the same data protection obligations set out in the contract or legal act between the controller and the initial processor must be imposed on the sub-processor through a contract or legal act.

(5) Where the sub-processor fails to fulfil its data protection obligations, the initial processor remains fully liable to the controller for the performance of those obligations.

(6) The processor must act only on the controller's instructions and assist the controller in complying with its obligations under this Act, including assisting with inspections.

(7) At the controller's choice, the processor must erase or return all personal data to the controller at the end of the provision of services related to processing, unless the law requires the retention of personal data.

28. Data protection by design and default

(1) Before processing personal data, controllers and, where applicable, processors must assess the potential impact on the fundamental rights and freedoms of data subjects and design the data processing to prevent or minimise risks to those rights.

(2) Controllers and processors must implement technical and organisational measures that account for the right to data protection at all stages of data processing.

(3) Data protection requirements must be integrated not only into the technology used for processing personal data but also into related work practices, management policies, and procedures.

(4) When setting technical requirements for default settings, controllers and processors must choose privacy-friendly configurations to ensure that the use of applications and software does not infringe the rights of data subjects.

(5) Controllers and processors must avoid processing more personal data than necessary to achieve the legitimate purpose. Measures must ensure that, by default, personal data is not accessible to an indefinite number of people without the data subject's intervention.

29. Security of processing

(1) To protect the rights and freedoms of data subjects, controllers and processors must implement appropriate technical and organisational measures to safeguard personal data and special categories of personal data from accidental or unauthorised access, use, loss, damage, alteration, disclosure, or destruction during transmission, storage, or processing.

(2) The measures required under subsection (1) must consider the nature of the personal data, the potential adverse consequences for data subjects, the state of technological development, and the cost of implementation, balanced against the potential risks to the data subject. Such measures may include –

(a) pseudonymisation of personal data;

(b) encryption of personal data;

(c) ensuring the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;

(d) restoring the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(e) regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(3) Controllers and processors must ensure that any person or third party acting under their authority and with access to personal data is aware of and complies with relevant security measures and does not process personal data except under the controller's or processor's instructions, unless required by law.

(4) The Commission may issue guidelines on appropriate security measures to ensure compliance with this Act.

30. Records of processing operations

(1) Controllers and processors must maintain a written record of processing activities under their responsibility, including in electronic form.

(2) The record must include the following information –

(a) the name and contact details of the controller and, where applicable, the joint controller and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and the categories of personal data;

(d) the categories of recipients to whom personal data has been or will be disclosed, including recipients in third countries or international organisations;

(e) the intended retention period for the data in relation to the specific processing purpose, and until the data is erased; and

(f) a general description of the technical and organisational security measures referred to in section 28.

31. Data protection impact assessment

(1) Where the processing of personal data is likely to result in a high risk to the fundamental rights and freedoms of data subjects, the controller, and where applicable, the processor, must carry out an assessment before commencing the processing and design the processing to prevent or minimise such risks.

(2) An assessment as referred to in subsection (1) is particularly required in cases involving –

(a) systematic and extensive evaluation of personal aspects relating to individuals based on automated processing, including profiling;

(b) large-scale processing of special categories of personal data; and

(c) systematic large-scale monitoring of publicly accessible areas.

(3) The assessment shall include at least –

(a) a description of the envisaged processing operations and the context and purposes of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purpose pursued;

(c) an assessment of the likely impact of the processing on the rights and freedoms of a data subject; and

(d) the measures envisaged to address potential risks, including safeguards, security measures, and mechanisms to protect personal data.

(4) The Commission shall establish and publish a list of processing operations that require a data protection impact assessment.

32. Obligations relating to personal data breaches

(1) The controller must notify the Commission without undue delay and no later than 72 hours after becoming aware of a personal data breach, unless the breach is unlikely to result in a high risk to the rights and freedoms of data subjects.

(2) Where a notification is not made within 72 hours, the controller must provide reasons for the delay, which the Commission may consider in determining compliance with this Act..

(3) Where a processor becomes aware of a personal data breach, they must notify the controller without undue delay, regarding any breach affecting the personal data processed on behalf of the controller

(4) The Notification under subsection (1) must include –

(a) a description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects affected;

(b) the likely consequence of the breach;

(c) the measures taken or proposed by the controller to address the breach, including measures to mitigate its potential adverse effects; and

(d) the metadata of the breach, including the time, location, duration, and data subject involved.

(5) The controller must document any personal data breach, including all relevant facts, its effects, and the remedial actions taken and this documentation must enable the Commission to verify compliance with this provision.

(6) The Commission shall develop and publish guidelines on handling data breaches and establish a mechanism for reporting such breaches

33. Personal data breach notification to data subjects

(1) Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the controller must notify the data subject without undue delay.

(2) The notification to the data subject must describe, in clear and plain language, the nature of the breach and recommend measures to address the breach, including, where appropriate, actions to mitigate its potential adverse effects.

(3) Notification to the data subject is not required where –

(a) controller has implemented appropriate technical and organizational protection measures to the personal data affected by the breach, particularly those that render the data unintelligible to unauthorised persons, such as encryption, as long as no known vulnerability in that encryption standard has been globally established;

(b) controller has taken measures to ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; or

(c) notification would involve disproportionate effort, and the controller has made a public communication or taken similar measures to inform data subjects in an equally effective manner.

34. Designation of the data protection officer

(1) The controller and processor must designate a data protection officer in the following cases –

(a) when processing is carried out by a public authority, service, agency, or other body, except for courts acting in their judicial capacity;

(b) when the core activities of the controller or processor involve regular and systematic monitoring of data subjects on a large scale, by the nature, scope, or purposes of the processing; or

(c) when the core activities of the controller or processor involve large-scale processing of special categories of data.

(2) A single data protection officer may be designated for several public authorities, services, agencies, or bodies, considering their organisational structure and size.

(3) The data protection officer must–

(a) inform and advise the controller, including the highest executives, the processor, and employees involved in processing, of their obligations under this Act;

(b) monitor compliance with this Act and the controller's or processor's policies on personal data protection, including assigning responsibilities, raising awareness, training staff involved in processing, and conducting audits;

(c) provide advice on data protection impact assessments when requested and monitor their performance; and

(d) cooperate with and act as the contact point for the Commission.

(4) The data protection officer may be internal or external to the data controller and must have knowledge in the field of data protection and in performing their tasks, the officer must consider the risks associated with processing operations, including the nature, scope, context, and purposes of the processing.

(5) The controller and processor must ensure the data protection officer's independence in performing their duties and ensure their involvement in important decisions related to data processing.

(6) The controller and processor must communicate the data protection officer's contact details to the Commission and provide a means for data subjects to contact the officer.

35. Cooperation with the Commission

(1) The controller, processor, and, where applicable, their representatives must cooperate with the Commission in the performance of its tasks.

(2) At the request of the Commission, the controller and processor must provide any information and records necessary for monitoring processing operations.

PART VI – EXCEPTIONS

36. Exceptions

(1) An exception to the provisions of this Act is permitted only when provided for by law, for a legitimate purpose, and in respect of fundamental rights and freedoms

and any exception must be a necessary and proportionate measure in a democratic society for the protection of –

(a) national security;

(b) defence;

(c) public safety;

(d) important economic and financial interests of the state;

(e) the impartiality and independence of the judiciary of The Gambia;

(f) the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties;

(g) other essential objectives of general public interest provided by law; or

(h) the protection of the data subject or the rights and fundamental freedoms of others, particularly the freedom of expression.

(2) The legislative measures referred to in subsection (1) must be accessible to data subjects, enabling them to reasonably foresee the exceptions and their consequences. Such measures must include specific provisions regarding –

(a) the purpose or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions;

(d) safeguards against abuse or unlawful access or transfer;

(e) a description of the controller or categories of controllers;

(f) the storage period and applicable safeguards, considering the nature, scope, and purposes of the processing; and

(g) the data subject's right to be informed about the restriction, unless such notification would undermine the purpose of the restriction.

(3) The use of exceptions and restrictions must be subject to objective and adequate safeguards to prevent arbitrary application and ensure legality.

(4) A restriction must be documented by the controller and made available to the Commission upon request.

PART VI – TRANS BORDER FLOWS OF PERSONAL DATA

37. Transfer of personal data outside the jurisdiction of The Gambia

(1) Cross-border transfers of personal data to other countries or international organisations are permitted when an appropriate level of protection is ensured, for legitimate purposes, and with mutual benefit to both jurisdictions and can be achieved through –

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

(b) ad hoc or standardised safeguards provided by legally binding and enforceable instruments adopted by the Commission and implemented by those involved in the transfer and further processing of personal data.

(2) The controller must assess the appropriate level of protection provided by the receiving country or international organisation, taking into account all circumstances surrounding the transfer and any guidance issued by the Commission and particular consideration must be given to –

(a) the nature of the personal data being transferred;

(b) the purpose and duration of the transfer;

(c) the data protection laws, both general and sectoral, in force in the receiving country or international organisation; and

(d) the recipients to whom the personal data is transferred, disclosed, or made accessible.

(3) The Commission must be involved in assessing whether the criteria for cross-border transfers are met, ensuring compliance with the principles outlined in section 4.

(4) The controller or processor must document the assessment of appropriate safeguards or criteria referred to in subsections (2) and (3).

(5) Upon request, the controller must provide the Commission with all relevant information regarding the transfers referred to in subsection (3). The Commission may request the controller to demonstrate the effectiveness of the safeguards or the existence of the criteria in subsections (2) and (3).

(6) To protect the rights and freedoms of data subjects, the Commission may prohibit or suspend transfers to other countries or international organisations, or impose additional conditions beyond those outlined in this section.

PART VIII – INFORMATION COMMISSION

38. Information Commission

(1) The Information Commission, established under the Access to Information Act shall also be responsible for data protection matters under this Act, in addition to its powers conferred by that law.

[Act No. 10 of 2021]

(2) The Commission shall act with complete independence and impartiality in performing its duties and exercising its powers. It shall not be subject to the control or direction of any other person or authority and shall neither seek nor accept external instructions unless in accordance with the law.

(3) The Commission shall recognise and treat the protection of personal data and privacy as a fundamental human right.

39. Composition of the Commission

The Commission established under the Access to Information Act must include a commissioner specialised in Personal Data Protection.

[Act No. 10 of 2021]

40. Functions of the Commission

(1) The Commission shall –

(a) monitor and ensure compliance with this Act and any regulations and statutory guidance made under it;

(b) promote public awareness and understanding of the provisions of this Act, particularly informing data subjects about their rights under this Act;

(c) address processing activities related to children and other vulnerable groups;

(d) promote awareness among controllers and processors of their obligations under this Act;

(e) issue opinions, either on its own initiative or at the request of a person with a legitimate interest, on matters related to the fundamental principles of data protection and privacy in the context of this Act;

(f) monitor the application of this Act and relevant developments, particularly in information and communication technologies and commercial practices, as they impact data protection and privacy;

(g) submit to the Court any legislative or administrative act that is not compliant with the principles of data protection and privacy as outlined in the Constitution of The Gambia and international human rights treaties to which The Gambia is a signatory;

(h) advise the President, the National Assembly, the Government, and other institutions on matters related to the right to data protection and privacy;

(i) conduct inquiries and investigations either on its own initiative or at the request of a data subject or any interested party;

(j) receive complaints lodged against a controller or processor by a data subject or their representative, through various channels such as direct, post, electronic means, or in person;

(k) investigate complaints and inform the complainant of the progress and outcome of the investigation within a reasonable period;

(l) explain to a data subject how to pursue a complaint if the Commission fails to respond or act on a request within three months of receiving it;

(m) establish and maintain a list of processing operations that require a data protection impact assessment;

(n) issue guidance on appropriate security measures and compliance with this Act;

(o) perform functions related to trans-border transfers of personal data under section 37(1)(b);

(p) develop and publish guidance on data breaches and establish a mechanism for reporting personal data breaches;

(q) keep internal records of infringements of this Act;

(r) cooperate with other supervisory authorities, share information, and participate in international negotiations on data protection matters as necessary to fulfil its duties under this Act; and

(s) prepare and publish an annual report outlining its activities, progress, challenges, and similar indicators.

(2) The tasks of the Commission shall be performed free of charge for data subjects.

(3) The Commission may refuse to act on requests that are manifestly unfounded or excessive, particularly if they are repetitive.

(4) The Commission may refuse requests that are not compatible with its powers or that do not comply with the provisions of this Act.

(5) The Commission bears the burden of proving that a request is manifestly unfounded or excessive.

(6) The Executive Secretary and staff of the Commission are bound by a duty of confidentiality and professional secrecy, both during and after their term of office, regarding any confidential information, including personal data, obtained in the course of their duties.

(7) Subsection (6) does not apply if the information is no longer confidential or has been declassified before any disclosure by the Executive Secretary or staff.

41. Powers of the Commission

In addition to its powers under the Access to Information Act, the Commission shall have the authority to investigate, intervene, and enforce the provisions of this Act and such powers include the ability to –

(a) request information, including records, copies, extracts of data, and oral or written explanations from controllers, processors, or their employees;

(b) enter and search a premise or a data processing equipment;

(c) observe and document the data processing activities;

(d) issue opinions or guidelines on the processing of personal data;

(e) issue decisions concerning violations of this Act;

(f) assist individuals to exercise their rights under this Act;

(g) impose administrative sanctions and monetary fines; and

(h) institute legal proceedings or bring violations of this Act to the attention of the competent judicial authorities of The Gambia.

[Act No. 10 of 2021]

42. Penalties and fines imposed by the Commission

(1) The Commission may impose the following penalties on controllers or processors failing to comply with the obligations of this Act –

(a) a corrective warning for non-compliance;

(b) a formal enforcement notice requiring the controller to cease non-compliance within a specified deadline, which may be limited to five days in urgent cases;

(c) a restriction of processing until the lawfulness of processing is established; and

(d) a financial penalty, calculated by the Commission;

(2) In cases of serious and immediate violations of a data subject's individual rights, the Commission may –

(a) impose a ban on the processing of personal data, particularly regarding international transfers that do not provide an equivalent level of data protection as required by this Act; or

(b) temporarily or permanently restrict the processing of, and access to, personal data.

(3) Decisions, penalties, and fines imposed by the Commission may be appealed to the High Court of The Gambia within thirty days of receiving the notification of the decision.

43. Cooperation between Data Protection Supervisory Authorities

(1) The Commission shall participate in international cooperation with other Data Protection Supervisory Authorities and networks of Supervisory Authorities.

(2) The Commission shall carry out the necessary data protection functions to fulfil international obligations arising from international data protection agreements or instruments.

(3) The Commission shall collaborate with other regulatory bodies in The Gambia to promote an effective regulatory environment and minimise duplicative or conflicting regulatory requirements and activities.

PART XI – MISCELLANOUS

44. Funds of the Commission

(1) The Commission shall be provided with sufficient human, technical, and financial resources, as well as the necessary premises and infrastructure, to ensure -

(a) its financial independence;

(b) the effective performance of its tasks; and

(c) the exercise of its powers, including those related to international cooperation.

(2) The Commission shall have the necessary resources and independence to employ skilled staff and build internal capacity.

45. Regulations

The Minister may make regulations prescribing matters -

(a) required or permitted by this Act to be prescribed; or
(b) necessary or convenient to be prescribed for carrying out or giving effect to this Act.

DATA PROTECTION AND PRIVACY BILL, 2024

OBJECTS AND REASONS

This Bill seeks to enhance substantial provisions with respect to Data Protection and Privacy and to establish the basic principles underlying the lawful processing of data, the rights of data subjects, the legal obligations of controllers and processors, trans-border data flows.

The Bill defines offences, penalties as well as exceptions and empowers the law enforcement agencies and establishes regulatory oversight mechanisms for the processing of personal data in promoting and protecting human rights and fundamental freedoms of individuals and in particular, the rights to privacy in accordance with the provisions of the Constitution of The Republic of The Gambia

……

Hon. Dr. Ismaila Ceesay

Minister of Information, Media and Broadcasting Services