Draft
T.T.F.
04.06.2025

DIGITAL SERVICES BILL, 2025
(Published on ,2025)

MEMORANDUM

1. A draft of the above Bill, which is intended to be presented to the National Assembly, is set out below.

2. The objective of the Bill is to enact the Digital Services Act to address challenges in developing digital services in Botswana and to accelerate Botswana's digital transformation. The Act will provide for the governance structures that will push the Digital Transformation Agenda, facilitate the development of quality standards, the enforcement of the interoperability of infrastructure and systems and the inclusivity of the citizens of Botswana in digital transformation.

3. To this end, the Bill –

(a) in Part I, provides for the definition of terms used in the law. This Part further provides that the law will apply to both public and private bodies that provide digital services and that carry out their businesses into or from Botswana, irrespective of the physical location from which the activity is carried out. The Part further provides that the law shall not apply to the provision of digital services by or on behalf of the State, to the extent necessary, where it involves national security, defence or public safety;

(b) in Part II, provides for the guiding principles for the provision of digital services. These guiding principles include, the need to focus digital services on the needs of the public and businesses in the delivery of services, the need to drive digital transformation through the development and utilisation of innovative design and integrated business processes which are streamlined, collaborative, and public-focused for the enhancement of service delivery, e.t.c.;

(c) in Part III, provides for the establishment of the Digital Transformation Coordination Office by law. The Office is currently established administratively under the Ministry of Communications and Innovation. The establishment of the Office by law will furnish the Office with the necessary powers of enforcement and implementation of this law. The Part therefore provides for the functions of the Office, amongst others, to be the regulation of digital services in Botswana and to develop and enforce strategies and standards that enhance provision and usage of digital services;

(d) in Part IV, provides for how digital services are to be regulated in terms of this law. The Part therefore provides for obligations on public and private bodies to develop accessible digital platforms for the provision of digital

services, the establishment of a Public Key Infrastructure for use by public and private bodies to ensure secure communication online, verify identities online and ensure data integrity. The Part further places an obligation on the Ministry responsible for national registration to develop a digital platform to enable the verification of identities online by issuing unique identification numbers to both natural and legal persons. The Part further provides that where any law requires a payment to be made or received, the requirement of the law is fulfilled, if the payment is made or received by secure electronic means. The Part further places an obligation on public and private bodies to keep their records in electronic form and that a public or private body shall, in undertaking an administrative procedure or public function by digital means, ensure that the documents to be presented in accordance with the procedure or function, shall be submitted by digital means. The Part further provides that a public or private body may implement joint automated procedures with other public or private bodies to enable data processing in or from a database. The Part further provides for the Office to develop and maintain a secure platform that will allow access for public bodies to exchange information and data sharing between systems for the provision of digital services;

(e) in Part V, provides for the Office to develop and coordinate a national Open Data Policy. The Part further provides for a public body which avails public data assets, to publish such assets as machine-readable and electronic data and further that, open data assets published by or for a public body shall be made available under an open licence. The Part further provides that the Coordinator, shall develop and maintain an Enterprise Data Inventory, in order to develop a clear and comprehensive understanding of the data assets in the possession of the public body;

(f) in Part VI, provides that public or private body shall ensure that security measures and safeguards are embedded and adhered to in the provision of digital services in line with relevant laws and policies; and

(g) in Part VII, provides for Miscellaneous provisions including a clause which empowers the Office to conduct periodical audits on public and private bodies to ensure that there is compliance with the standards set up by the Office. The Part further provides for the offences and penalties for any contravention of the provisions of this law and transitional arrangements that provide for a grace period of 24 months for public and private bodies to meet the requirements and standards set by the law.

DAVID TSHERE
Minister of Communications and Innovation.

ARRANGEMENT OF SECTIONS

SECTION

PART I – *Preliminary*

1. Short title and commencement
2. Interpretation
3. Application of Act
4. Conflict with other laws

PART II – *Guiding Principles*

5. Guiding principles for digital services

PART III – *Digital Transformation Coordination Office*

6. Establishment of Digital Transformation Coordination Office
7. Directions by Minister
8. Functions of Office
9. Cooperation with public and private bodies

PART IV – *Control of Digital Services*

10. Digital Government Plan and Digital Services Plans
11. Electronic access to digital services
12. Establishment of Public Key Infrastructure
13. Online unique identification
14. Electronic means of payment
15. Required documentation and data sharing
16. Electronic record keeping
17. Digitisation of records
18. Electronic filing of documents
19. Access to files and records
20. Joint automated procedures
21. Information gateway
22. Requirements pertaining to provision of data
23. Electronic *Gazette*

PART V – *Open Data*

24. Open data
25. Requirements for open data and open licences
26. Promotion of innovation
27. Enterprise Data Inventory
28. Information resource management
29. Information dissemination
30. Technology portal

31. Repository

PART VI- *Information Security*

32. Information security

PART VII – *Miscellaneous Provisions*

33. Audit of public and private bodies
34. Exemption from liability of officers of the Office
35. Exemptions
36. Appeals
37. Offences and penalties
38. Regulations
39. Transitional arrangements

A BILL

-entitled-

An Act to provide for the regulation of digital services; to enhance the management and promotion of digital services and processes; to establish the Digital Transformation Coordination Office which shall be responsible for the formulation of digital services standards and provide for its functions; facilitate access to digital services to improve service delivery, administrative functions and productivity in order to enhance public access to digital services and information; and provide for matters connected with, or incidental, to the foregoing .

PART I - *Preliminary*

Short title and commencement

1. This Act may be cited as the Digital Services Act, 2025, and shall come into operation on such date as the Minister may, by Order published in the *Gazette*, appoint.

Interpretation

2. In this Act, unless the context otherwise requires –

"authentication" means the process of confirmation or validation of the identity of a data source or identity;

"authenticity" means the assurance that a message, transaction or other exchange of information is from the author or service the message transaction or other exchange of information purports to be from;

"Coordinator" means the Digital Transformation Coordinator appointed in terms of

"data" has the same meaning assigned to it under the Data Protection Act;

Cap. 43:11

"data controller" has the same meaning assigned to it under the Data Protection Act;

"data subject" has the same meaning assigned it under the Data Protection Act;

"digital services" means any service that is delivered or accessed through digital means;

"electronic governance" means the use of information and communication technology

to enhance work efficiency and improve service delivery in order to meet the needs of the public in a responsive and transparent manner and "e-government" shall be construed accordingly;

"e-government service" means any service provided by electronic means by a public body;

"electronic signature" has the same meaning assigned to it under the Electronic Communications and Transactions Act;

"electronic transactions" has the same meaning assigned to it under the Electronic Communications and Transactions Act;

"information system" has the same meaning assigned to it under the Electronic Communications and Transactions Act;

"Office" means the Digital Transformation Coordination Office;

"public body" means any office, organisation, establishment or body created by or under any enactment or under powers conferred by any enactment; or any organisation, trust, company or body where public moneys are used or government has equity shareholding in it, and includes –

(a) a Ministry or Government Department;

(b) a local authority;

(c) land board;

(d) Statutory body; and

(e) any company registered under Companies Act being a company in which the Government or an agency of the Government through holding of shares or otherwise, is in a position to

Cap. 42:01

direct the operations of that company;

"Public Key Infrastructure (PKI)" means a framework for creating a secure method for exchanging information based on public key cryptography;

"public register" means a register required to be maintained by a public body under any other written law;

"private body" means" any office, organisation, establishment, body, trust, company or any legal entity which provides goods and/or services in Botswana, irrespective of whether payment is required, where public moneys are not used or government has any shareholding; and

Cap. 01:02

"unique identifier" means, for natural persons an identity number as defined in the National Registration Act and for legal entities a number or alpha numerical that distinguishes entities, used for the purpose of identifying and authenticating users within the digital services platforms.

Application of Act

3. (1) This Act shall apply to public and private bodies in the provision of digital services that carries out business into or from Botswana, irrespective of the physical location from which the activity is carried out.

(2) This Act shall not apply to the provision of digital services by or on behalf of the State, to the extent necessary, where it involves national security, defence or public safety.

Conflict with other laws

4. In the event of a conflict or inconsistency between the provisions of this Act and any other law on digital services, the provisions of this Act shall take precedence.

PART II – *Guiding Principles for Digital Services*

Guiding principles for digital services

5. The guiding principles for the provision of digital services shall include the following –

(a) digital services shall focus on the needs of the public and businesses in the delivery of services;

(b) driving digital transformation through the development and utilisation of innovative design and integrated business processes which are streamlined, collaborative, and public-focused for the enhancement of service delivery;

(c) innovative application of solutions to promote efficiency and create opportunities to evaluate and eliminate redundant steps associated with conventional processes;

(d) integrated provision of digital services which recognises the unique roles and capabilities of public bodies;

(e) sharing of information among public and private bodies electronically which avoids information duplicity;

(f) sharing of infrastructure among public and private bodies to promote innovation and equitable access to resources;

(g) ensuring information security for digital services;

(h) prudent and responsible use of public resources in the implementation of digital services; and

(i) collaboration between public and private bodies for the promotion and optimisation of sustainable resource utilisation.

PART III – *Digital Transformation Coordination Office*

Establishment of Digital Transformation Office

6. (1) There is hereby established, in accordance with the laws governing the public service, an Office to be known as the Digital Transformation Coordination Office, which shall be responsible for the regulation of digital services in Botswana.

Cap. 26:01

(2) Subject to the Public Service Act, the President shall appoint a Digital Transformation Coordinator on such terms and conditions as may be specified in the instrument of appointment.

(3) The other officers of the Office shall be appointed in accordance with the Public Service Act

Directions by Minister

7. (1) The Minister may give the Office directions of a general or specific nature regarding the exercise of its powers and the performance of its functions, which directions shall not be inconsistent with this Act or with the obligations of the Office, and the Office shall give effect to any such direction.

(2) The Coordinator shall, subject to the direction of the Minister, be responsible for the administration of the Office.

Functions of Office

8. The functions of the Office shall be to –

(a) develop, promote and manage digital service policies and programmes;

(b) develop and enforce strategies and standards that enhance provision and usage of digital services;

(c) promote collaboration in the provision of digital services;

(d) delivery of digital services to the public by integrating related functions and systems;

(e) promote access to digital services across multiple channels;

(f) promote digital services education and utilisation;

(g) undertake research on information and communication technologies to promote digital services;

(h) develop supportive and enabling shared infrastructure guidelines to ensure equitable access to effective and appropriate provision of digital services;

(i) oversee the design and development of appropriate applications for the support of e-governance and information management systems;

(j) provide high level blueprint to guide the development and provision of digital services;

(k) provide technical support and advice to various digital services projects, programmes and interventions;

(l) undertake public protection measures in the consumption of digital services;

(m) develop and oversee the implementation of a National Digital Services Strategic Plan;

(n) develop and implement the National Digital Government Plan;

(o) establish a structured digital services stability management plan;

(p) ensure that public data is preserved in a secure designated area for service continuity;

(q) biennially carry out such studies on the implementation of this Act by public bodies, including an update on the state of implementation of digital services by public bodies and publish such results;

(r) provide advice, information or policy proposals to the Minister on matters relating to digital services; and

(s) carry out other functions that are necessary for the performance of its functions under this Act.

Cooperation with other bodies

9. (1) In the exercise of its functions, the Office shall cooperate with public and private bodies in the implementation of this Act.

(2) Public and private bodies shall accord the Office such assistance as may be necessary to ensure the proper discharge of the functions of the Office.

(3) Subject to the provisions of subsection (1), the Officer shall in the performance of its functions promote digital service, through international cooperation.

PART IV – C*ontrol of Digital Services*

Digital Government Plan and Digital Service Plans

10. (1) The Coordinator shall develop and implement a Digital Government Plan for public bodies.

(2) The Digital Government plan shall include –

(a) strategies and projects for implementing digital services, including a priority plan for electronic services;

(b) strategies and projects for the management of key digital services infrastructure identified by the Office;

(c) harmonisation requirements for implementation of the strategies and projects under paragraph *(a)*; and

(d) any other digital services projects related to the implementation and operation of these services.

(3) Private bodies shall develop Digital Service Plans that shall adhere to the standards set out in this Act and under the guidance provided by the Coordinator.

Electronic access to digital services

11. A public or private body shall establish an accessible electronic platform to enable the provision of digital services.

Establishment of Public Key Infrastructure

12. (1) The Office shall establish a Public Key Infrastructure for use by public or private bodies.

(2) The Public Key Infrastructure shall, among others –

(a) ensure secure communication online;

(b) verify identities online; and

(c) ensure data integrity.

Online unique identification

13. (1) The Ministry responsible for national registration shall provide a digital online platform to verify the unique identifiers for natural persons.

(2) The Ministry responsible for national registration, shall on an application by a legal person or at request of a public or private body on behalf of a legal

person, assign a unique identifier to the legal person, for the purposes of electronic validation of that person's identity.

Electronic means of payment

14. (1) Where a law requires a payment to be made or received, the requirement of the law is fulfilled, if the payment is made or received by secure electronic means and complies with the relevant law.

(2) Where a law requires the issuance of a receipt as proof of payment, the requirement is fulfilled if the receipt is in electronic form and is accessible and intelligible, so as to be usable for subsequent references.

Required documentation and data sharing

15. (1) A public or private body shall, in undertaking an administrative procedure or public function by digital means, ensure that the documents to be presented in accordance with the procedure or function, shall be submitted by digital means.

(2) A public or private body may determine which format of electronic submission is permissible for the purposes of that body.

(3) Subject to the provisions of the Data Protection Act, a public or private body with the consent of a data subject, may retrieve the required documentation originating from one public or private body for processing and usage of the personal data for that purpose.

(4) Where information has been shared for public function purposes, it may be reshared further by another public body for another public function.

(5) A public body shall avoid the collection of information by a public body that is already held by another public body.

(6) The Office may operate a system for sharing data collected and managed through electronic systems for the provision of digital services.

Electronic record keeping

16. (1) A public or private body shall keep its records in electronic form.

(2) A public or private body shall ensure that where records are kept in an electronic form, appropriate technical and organisational measures are implemented in accordance with the technological standards as shall be determined by the Coordinator, to ensure that the principles of orderly

record keeping and legal requirements for duration of maintenance of records are observed.

(3) Where a public body is mandated to keep a register under any law, it shall ensure that such register is kept in an electronic format in accordance with this Act.

(4) The Office shall develop and maintain a digital services integrity register, in such manner and form as may be prescribed, which shall record the availed digital services provided by public and private bodies.

Digitisation of documents

17. (1) A public or private body shall, when digitising its records, ensure that the digitisation is in accordance with the technological standards determined by the Coordinator.

(2) A public or private body shall, when digiting its records, ensure that the pictorial and text content of the electronic document corresponds to the paper documents.

(3) The Coordinator may, on the request of a public or private body, waive the requirement to digitise its documents, where the digitisation would entail disproportionate efforts.

Electronic filing of documents

18. (1) Where a public or private body pursuant to this Act or any other law, accepts the filing of documents, or requires that documents be created, written or retained, issues a permit, licence or provides for a manner of payment, shall –

(a) accept the filing of such documents in electronic form;

(b) issue such permits, licences or approvals in electronic form; or

(c) make or receive payment in electronic form.

(2) A person shall not, where a law allows information to be presented or retained in electronic form, demand that the information that person presents be received in electronic form by a public or private body otherwise than as specified or required by that public or private body.

Access to files or records

19. A public or private body shall, where a right to inspect a file or record exists, grant access to files by –

(a) displaying the electronic documents on a screen;

(b) transmitting electronic documents;

(c) permitting electronic access to the content of the files; or

(d) providing a print-out of the documents concerned.

Joint automated procedures

20. (1) A public or private body may implement joint automated procedures with other public or private bodies to enable data processing in or from a database.

(2) Where joint automated procedures under subsection (1) are also intended to enable data retrieval by other bodies, the retrieval procedures, shall in relation to the protection of personal data, be implemented in accordance with this Act and the Data Protection Act.

(3) The participation of other public or private bodies in joint automated procedures shall only be undertaken, where it is appropriate with due regard to a data subject's legitimate interests and the tasks to be performed by the participating public or private bodies.

(4) A public or private body shall, before establishing or effecting substantial changes to a joint automated procedure, specify the following, in writing –

(a) the procedure to be applied and the bodies responsible for defining, amending, developing and complying with organisational and technical specifications for the joint automated procedure; and

(b) the participating bodies responsible for ensuring the legality of collecting, processing and using data, respectively.

(5) A public or private body under subsection (1) shall appoint an authorised officer, who shall coordinate the implementation of this section.

(6) The authorised officer under subsection (5) shall cause to be prepared guidelines for coordination of joint automated procedures, which guidelines shall be made available by the public or private body, for inspection by the Office.

(7) Subject to the provisions of this Act, the Data Protection Act, the Cybercrime and Computer Related Crimes Act, the Cybersecurity Act and any other relevant law, a public or private body may commission another body to collect, process and use personal data for the joint automated procedure.

Cap. 08:06
Act No. of 2025

Information gateway

21. (1) For the purposes of this section, "information gateway" means a secure platform allowing access for public bodies to exchange information and data sharing between systems for provision of digital services.

(2) The Office shall develop and administer the information gateway.

(3) A public body providing information through the gateway shall ensure the relevance and clarity of the information, and that it is organised in a user-centric manner.

(4) The Office may establish the requirements and procedures for access to the information gateway by public bodies.

Electronic Gazette

22. For the purposes of this Act, the Office of the Government Printer shall develop and maintain an electronic *Gazette.*

(2) Where any law provides that any rule, regulation, bye-law, notification or any other matter shall be published in the *Gazette,* then, that requirement shall be deemed to have been satisfied if that rule, regulation, order, bye-law, notification or any other matter is published in the *Gazette* or *e-Gazette,* except that, where any rule, regulation, order, bye-law, notification or any other matter is published in the *Gazette* or *e-Gazette,* the date of publication shall be deemed to be the date of the *Gazette* which was first published in any form.

PART V – *Open Data*

Open data

23. (1) The Office shall develop and coordinate the implementation of a national Open Data Policy.

(2) Where a public or private body employs publicly accessible networks to make data available, that public or private body shall use a machine-readable and electronic format as a general principle.

Requirements for open data and open licences

24. (1) A public body which avails public data assets, shall publish such assets as machine-readable and electronic data.

(2) Subject to the provisions of any law and to such extent as practicable, open data assets published by or for a public body shall be made available under an open licence.

(3) Public and non-public data assets maintained by public bodies shall be stored in an open format.

Promotion of innovation

25. A public body may engage with a private body or another public body to explore opportunities to leverage the public data assets of the public body, in a manner that may provide new opportunities for innovation in the public and private sector.

Enterprise Data Inventory

26. (1) A public body, in consultation with the Coordinator, shall develop and maintain an Enterprise data inventory, in order to develop a clear and comprehensive understanding of the data assets in the possession of the public body

(2) A public body shall ensure that the Enterprise Data Inventory accounts for any data asset created, collected, under the control or direction of, or maintained by the public body, with the goal of including all data assets, to such extent as is practicable.

(3) The Enterprise Data Inventory shall include each of the following information –

(a) data assets used in the information systems of public bodies, including program administration and statistics generated by applications, devices, networks, facilities, and equipment, categorised by source type;

(b) data assets created, maintained or shared by public bodies;

(c) data assets that can be made publicly available under the Access to Information Act, 2024.

(d) a description of whether the public body has determined that a data asset may be made publicly available and whether the data asset is available to the public;

(e) non-public data assets; and

(f) public data assets.

(3) The Coordinator shall issue standards for the Enterprise Data Inventory, including –

(a) requirements that the Enterprise Data Inventory includes a compilation of metadata about public body data assets; and

(b) criteria that a public body shall use in determining whether to make a particular data asset publicly available in a manner that takes into account -

(i) the expectation of confidentiality associated with a public data asset,

(ii) security considerations, including the risk that information in a public data asset in isolation does not pose a security risk but when combined with other available information may pose such a risk,

(iii) the cost and benefits to the public of converting the data into a manner that could be understood and used by the public,

(iv) the expectation that all data assets that would otherwise be made available under the Access to Information Act be disclosed; and

(v) any other considerations that the Coordinator determines to be relevant.

(4) Non-public data assets included in the Enterprise Data Inventory may be maintained in a non-public section of the inventory.

(5) A public body shall –

(a) make the Enterprise Data Inventory available to the public on a platform availed by the Office;

(b) ensure that access to the Enterprise Data Inventory and the data contained therein is consistent with the relevant laws;

(c) to the extent practicable, complete the Enterprise Data Inventory by the date to be determined by the Office; and

(d) add additional data assets to the Enterprise Data Inventory, not later than 180 days after the date on which the data asset is created or identified.

(6) A public body shall follow the standards set by the Coordinator issued pursuant to subsection (3) to make public data assets included in the Enterprise Data Inventory publicly available in an open format and under an open license.

Information resource management

27. (1) A public body shall, with respect to information resource management –

(a) improve the integrity, quality, and utility of information to all users within and outside the public body, by using an open format for any new public data asset created or obtained on the date to be determined by the Office;

(b) to the extent practicable, encourage the adoption of open format for all public data assets created or obtained before the commencement of this law;

(c) in consultation with the Coordinator, develop an open data plan that, at a minimum and to the extent practicable –

(i) requires the public body to develop processes and procedures that require each new data collection mechanism to use an open and machine-readable format, and

(ii) allow the public body to collaborate with private bodies, public bodies and members of the public for the purpose of understanding how data users value and use public data assets;

(d) identify and implement methods for collecting and analysing digital information on data asset usage by users within and outside of the public body;

(e) designate a point of contact within the public body to assist the public and to respond to quality issues, usability, recommendations for improvements, and complaints about adherence to open data requirements;

(f) develop and implement a process to evaluate and improve the timeliness, completeness, accuracy, usefulness, and availability of public data assets.

(g) update the open data plan at an interval determined by the Coordinator; and

(h) provide controls to avoid the dissemination and accidental disclosure of non-public data assets.

Information dissemination

28. (1) A public body shall, with respect to information dissemination –

(a) provide access to public data assets online;

(b) take the necessary precautions to ensure that the public body maintains the production and publication of data assets which are directly related to activities that protect the safety of human life or property; and

(c) engage the public in using public data assets and encourage collaboration by –

(i) publishing information on public data assets' usage in regular, timely intervals, at least once a year,

(ii) receiving public input regarding priorities for the analysis and disclosure of data assets to be published;

(iii) assisting civil society groups and members of the public working to expand the use of public data assets, and

(iv) develop and promote initiatives designed to create additional value from public data assets.

Technology portal

29. (1) The Coordinator shall maintain a platform as a point of entry dedicated to sharing public data assets with the public.

(2) The Coordinator shall determine, after consultation with a public body, the method to access public data assets published through the platform.

Repository

30. (1) The Office shall develop and maintain an online repository of tools, best practices, and schema standards to facilitate the adoption of open data practices, which shall include –

(a) regulation, policy, checklists and case studies related to open data; and

(b) the collaboration and the adoption of best practices across public bodies relating to the adoption of open data practices.

(2) The Coordinator may make guidelines for use of the data under this section, including commercial and non-commercial use, conditions of use and exclusion of liabilities and warranties.

PART VI – *Information Systems Security*

Information security

31. A public or private body shall ensure that security measures and safeguards are embedded and adhered to in the provision of digital services in line with relevant laws and policies.

PART VII – *Miscellaneous Provisions*

Audit of public and privatebodies

32. (1) The Office may conduct audits of a public or private body, for the purpose of evaluating compliance with the provisions of this Act.

(2) Subject to the provisions of subsection (1), an audit conducted under subsection (1) may be performed by independent auditor approved by the Coordinator.

(3) The Office shall, where an audit reveals that a public or private body has contravened any provision of this Act, notify the public or private body, in writing, the findings of the audit report, and consult, on the -

(a) action required to remedy the non-compliance; and

(b) period within which a public or private body shall take the remedial action.

Annual report

33. (1) The Office shall, within a period of six months after the financial year or within such longer period as the Minister may approve, submit, to the Minister, a comprehensive report of its operations during that year, and

the report shall be published in such manner as the Minister may require.

(2) The Minister shall lay the annual report of the Office in Parliament, within three months of its receipt.

Exemption from liability of officers of the Office

34. No liability, civil or criminal, shall attach to an officer of the Office, in respect of any loss arising from the exercise, in good faith by the officer of his or her function under this Act.

Exemptions

35. The Minister may by Order published in the Gazette exempt a public or private body from the provisions of this Act, taking into account the size of the entity, revenue turnover and nature of services provided by the entity.

Appeals

36. A person who is aggrieved by a decision of the Office given under this Act may, within 30 days from the date of the notification or communication of the decision to him or her, appeal against that decision to the High Court.

Offences and penalties

37. (1) A public or private body which, without lawful authority –

(a) discloses information provided to that public or private body for the purpose or during the course of delivery of digital services;

(b) publishes or discloses to any person otherwise than in the course of that person's duties, the contents of any documents, communication, or information which relates to, and which has come to that person's knowledge in course of that person's duties under this Act;

(c) having information which to such public or private body's knowledge has been published or disclosed in contravention of paragraph *(a)*, unlawfully publishes or communicates such information to any other person,

the public or private body commits an offence and is liable to pay to the Office, a civil penalty not exceeding 10 per cent of the net turnover of the public or private body for the previous financial year and where no net turnover for the previous financial year exists, 10 per cent of the gross revenue of the period of existence of the public or private body shall be used by the Office to determine the quantum of the civil penalty.

(2) A person who –

(a) forges, alters, damages, or deletes information for the purpose of interfering with the processing of such information;

(b) forges, alters, damages or uses an information system for the purpose of sharing of information without good cause;

(c) discloses or disseminates to the public, any method or program by which information can be altered or deleted;

(d) processes information without lawful authority or beyond the authority accorded,

commits an offence and is liable to a fine not exceeding P50 000 or to imprisonment to a term not exceeding three years, or to both.

Regulations

38. The Minister may make regulations for the better carrying out of the provisions of this Act.

Transitional arrangements

39. A public or private body which carried out digital services before the commencement of this Act and does not conform to the provisions of this Act, shall within a period of 24 months from the commencement of this Act, undertake such processes and activities to conform to the provisions of this Act.