

**THE ELECTRONIC GOVERNMENT BILL, 2021**

**MEMORANDUM**

The objects of this Bill are to—

- (a) enhance the management and promotion of electronic Government services and processes;
- (b) establish the Electronic Government Division in the Office of the President and provide for its powers and functions;
- (c) facilitate access to electronic Government services to improve service delivery, administrative functions and productivity in order to enhance citizens access to Government services and information; and
- (d) provide for matters connected with, or incidental, to the foregoing.

L. KALALUKA,  
*Attorney-General*



**THE ELECTRONIC GOVERNMENT BILL, 2021**

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY

*Section*

1. Short title and commencement
2. Interpretation
3. Application of Act

PART II

GUIDING PRINCIPLES OF E-GOVERNMENT

4. Guiding principles for e-government

PART III

ELECTRONIC GOVERNMENT DIVISION

5. Establishment of electronic Government Division
6. Functions of Division
7. National Coordinator and other staff

PART IV

CONTROL OF E-GOVERNMENT SYSTEMS AND SERVICES

8. Scope of application
9. National e-government plan
10. Electronic access to Government
11. Electronic means of payment
12. Required documentation and data sharing
13. Electronic record-keeping
14. Conversation and destruction of original paper documents
15. Access to files
16. Optimisation of administrative procedures and information on status of progress
17. Joint automated procedures
18. Requirements pertaining to provision of data
19. Electronic forms
20. Data protection

21. Identity and authenticity
22. Restriction on use of personal information
23. Non-disclosure of information provided to public body
24. Citizen card

PART V

INFORMATION SYSTEMS SECURITY

25. Information security
26. Security of information
27. Access to and sharing of information
28. Audit of public body

PART VI

PUBLIC SERVICE ELECTRONIC TRANSACTIONS

29. Electronic filing, electronic signature and issuing of documents by public body
30. Receipt of information by public body
31. Determination of originality of data message
32. Use and acceptance of electronic signature for public body
33. Electronic Gazette

PART VII

GENERAL PROVISIONS

34. Annual Reports
35. Geo-referencing
36. Prohibition of disclosure of information to unauthorised persons
37. Regulations

# A BILL

ENTITLED

**An Act to enhance the management and promotion of electronic Government services and processes; establish the Electronic Government Division in the Office of the President and provide for its powers and functions; facilitate access to electronic Government services to improve service delivery, administrative functions and productivity in order to enhance citizens access to Government services and information; and provide for matters connected with, or incidental, to the foregoing.**

ENACTED by the Parliament of Zambia.

Enactment

## PART I PRELIMINARY

1. This Act may be cited as the Electronic Government Act, 2021, and shall come into operation on the date appointed by the President by statutory instrument. Short title and commencement
2. In this Act, unless the context otherwise requires - “advanced electronic signature” has the meaning assigned to the words in the Electronic Communications and Transactions Act, 2021; Interpretation
- 10 “approved website” means a website approved by the Attorney-General for the publication of electronic legislation for the Republic; Act No. 4 of 2021

	“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;	
	“authentication” means the process of confirmation or validation of the identity of a data source or identity;	5
Act No. 4 of 2021	“certification authority” has the meaning assigned to the words in the Electronic Communications and Transactions Act, 2021;	
Cap. 1	“citizen” has the meaning assigned to the word in the Constitution;	10
	“citizen card” means the logical unit, independent of whether implemented on different technical components or not, combining an electronic signature with an identity link and the associated security data, functions and any existing data on representation;	15
	“court” means a court of competent jurisdiction;	
Act No. 3 of 2021	“data controller” has the meaning assigned to the Act No. 3 of 2021 words in the Data Protection Act, 2021;	
Act No. 3 of 2021	“data subject” has the meaning assigned to the words in the Data Protection Act, 2021;	20
	“Division” means the Electronic Government Division established under section 5;	
	“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	25
	“e-government” shall be construed accordingly;	
	“e-government service” means any public service provided by electronic means by any public body;	30
	“electronic service” includes the use of electronic means for interaction between citizens and government, including availing services from the government, understanding status of work in progress and accessing results of the process;	
Act No. 4 of 2021	“digital signature” has the meaning assigned to the words in the Electronic Communications and Transactions Act, 2021;	35

- “geographic information system” means an information system that involves locational data, including maps or other geo-spatial information resources;
- 5 “identity” means designation of a specific person by means of data which distinguishes that person from other persons including name, date of birth, place of birth, company name, alpha numerical or other unique identifying data designations;
- 10 “information security” means the state of being protected against the unauthorised use of information, especially electronic data or the measures taken to achieve this;
- “information system” means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages, and includes the internet;
- 15 “public body” has the meaning assigned to the words in the Public Finance Management Act, 2018; Act No. 1 of 2018
- “Public Key Infrastructure (PKI)” means a framework for creating a secure method for exchanging information based on public key cryptography;
- 20 “public officer” has the meaning assigned to the words in the Constitution; Cap. 1
- “public register” means a register required to be maintained by a public body under any other written law;
- 25 “public service” has the meaning assigned to the words in the Constitution; Cap. 1
- “source identification number “ means a number used to identify natural and legal persons and other data subjects which is attributable to the data subject to be identified and which, in the case of a natural person, also serves as the basis for generating sector-specific personal identifiers; and
- 30 “unique identity” means designation of a specific person by means of one or more features enabling that person to be distinguished from another data subject.

Application of Act	3. Subject to the other provisions of this Act, nothing in this Act prejudices, limits or restricts any other law regulating the dealings between the Government and the public.	
	<b>PART II</b>	
	GUIDING PRINCIPLES OF E-GOVERNMENT	5
Guiding principles for e-government	4. The guiding principles of e-government include the following:	
	(a) e-government shall focus on the needs of citizens and businesses in the delivery of services;	
	(b) development and utilisation of innovative design and transformational integrated business processes which are streamlined, collaborative, and citizen-focused for the enhancement of service delivery;	10
	(c) innovative application of solutions in order to reduce long-term operational costs and create opportunities to evaluate and eliminate redundant steps and processes and reduce cycle times associated with conventional processes;	15
	(d) integrated provision of e-government service which recognises the unique roles and capabilities of public bodies;	20
	(e) sharing of administrative information among public bodies which avoids information duplicity;	
	(f) protection of information held by a data controller used in accordance with the law;	
	(g) prudent and responsible use of public resources in the implementation of e- government activities; and	25
	(h) collaboration with the private sector for the promotion and optimisation of sustainable resource utilisation.	
	<b>PART III</b>	
	ELECTRONIC GOVERNMENT DIVISION	30
Establishment of electronic Government Division	5. (1) There is established the Electronic Government Division as a Division in the Office of the Division President which is responsible for the administration of this Act under the general direction of the President.	

(2) The Division shall, subject to the general direction of the President, be responsible for the coordination of e-government and information and communication technology matters in public bodies.

- 5     **6.** (1) The functions of the Division are to— Functions of  
Division
- (a) promote and manage e-government policies and programmes;
- (b) develop strategies and standards that enhance usage and application of information and communication technology innovations in the public sector;
- 10           (c) ensure that public data is preserved in a secure government designated area and backups in specified locations;
- (d) promote inter-government agency collaboration in providing e-government services, in order to improve the service delivery to citizens by integrating related functions and systems;
- 15           (e) promote information and communication technologies education and utilisation;
- (f) provide access to high quality Government information and services across multiple channels;
- (g) undertake research on information and communication technologies;
- (h) develop supportive and enabling shared infrastructure to ensure equitable access to effective and appropriate information and communication technologies;
- 25           (i) develop, disseminate and enforce quality assurance, security and other standards in the provision of information and communication technologies;
- (j) design and develop appropriate applications for the support of e-governance and other electronic services;
- (k) provide technical support to various information and communication technologies projects, programmes and interventions in public bodies;
- 35           (l) manage information and communication technology related service level agreements with service providers and clients;

- 
- (*m*) recommend the recruitment and placement of, and manage and supervise information and communication technology staff in public bodies;
- (*n*) oversee the design and implementation of information management systems, in public bodies and any other 5 institutions to which public funds are appropriated;
- (*o*) establish a coordinated official email communication and central information technology infrastructure for the effective implementation of the system;
- (*p*) implement an information communication and technology 10 development plan;
- (*q*) promote paperless transactions in the public service; and
- (*r*) carry out other functions relating to e-governance of information and communication technologies that are necessary for the performance of its functions under 15 this Act.
- (2) The Division shall, for the purposes of performing its functions under subsection (1)—
- (*a*) enforce the provisions of this Act and any prescribed standards of generally recognised e-government, 20 information and communication technology practices and uniform classification systems in public bodies;
- (*b*) monitor and assess compliance with this Act and any other relevant written law and take administrative action against a public body or refer it to a relevant institution 25 or law enforcement agency for a contravention of this Act;
- (*c*) assist public bodies in building their capacity for efficient, effective and transparent e-government services;
- (*d*) monitor and evaluate information systems and internal 30 controls in public bodies; and
- (*e*) develop policies and procedures relating to the proper management of information and communication technology systems and assets in the delivery of public services. 35

7. (1) The President, through the Civil Service Commission, shall appoint a National Coordinator of the Division who shall be a public officer. National Coordinator and other staff

(2) The National Coordinator is the chief executive officer of the Division and is responsible for the day- to-day management of the Division.

(3) The Civil Service Commission shall appoint other staff of the Division who are necessary for the implementation of the provisions of this Act.

10

PART IV

CONTROL OF E-GOVERNMENT SYSTEMS AND SERVICES

8. (1) This Act shall apply to the administrative activities by public bodies under any other written law in force in the Republic which are directly accountable to the Government. Scope of application

15 (2) This Act shall apply to the activities of a court or tribunal established under any other law.

9. (1) The National Coordinator shall develop a national e-government plan for the purposes of the National Planning and Budget Act, 2020. National e-government plan  
Act No. 1 of 2020

20 (2) The national e-government plan shall include—

- (a) strategies and projects for reducing paper documents in public bodies;
- (b) strategies and projects for the management of administrative information resources by public bodies;
- 25 (c) harmonisation requirements for implementation of the strategies and projects;
- (d) projects for installing an information and communications network among public bodies and securing safety;
- (e) medium and long term project plans; and
- 30 (f) other e-government projects related to the implementation and operation of e-government.

10. (1) A public body shall establish a point of access for the transfer of electronic documents, including documents provided with advanced electronic signature. Electronic access to Government

- Cap. 126  
Electronic means of payment
- (2) A public body shall in any administrative procedure or public function in which it is required to establish a person's identity by virtue of a legal provision or in which the public body considers identification to be necessary on other grounds, offer electronic proof of identity issued under the National Registration Act. 5
- 11.** (1) Where a law requires a payment to be made, the requirement of the law is fulfilled if the payment is made by electronic means and complies with any conditions imposed by the Government.
- (2) Where a law requires the issuance of a receipt of payment, 10 that requirement is fulfilled if the receipt is in electronic form and is accessible and intelligible so as to be usable for subsequent reference.
- (3) An information processing system used for standards relating to electronic transactions shall be sufficiently secured in 15 accordance with accepted technological standards at the time relating to authentication, integrity, availability and confidentiality to process electronic transactions including electronic banking, mobile banking, electronic funds transfers, point of sale, automatic teller machines and other related electronic transactions or systems 20 or as may be prescribed.
- (4) An organisation engaged in electronic payments, contracts and service provision shall meet security requirements in line with the relevant industry standards of the technology being offered by that organisation for electronic payments. 25
- (5) A public body shall, where a charge or other amount receivable arises in connection with an administrative procedure or public function carried out by electronic means, enable payment of that charge or other amount receivable by participating in at least one adequately secure payment procedure which is customary 30 in the area of electronic business transactions.
- Required documentation and datasharing
- 12.** (1) Where an administrative procedure or public function is carried out by electronic means, the documents to be presented may be submitted by electronic means, except where this contravenes a legal provision or where a public body requires the 35 submission of an original document.

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

(3) A public body may, with the consent of a data subject, as applicable, retrieve required documentation originating from another public body directly from the issuing public body, and the requesting public body and the providing public body may collect, process and use the necessary personal data for that purpose.

(4) In the absence of any legal provisions to the contrary, the consent granted under subsection (3) may be provided by electronic means and shall be documented.

(5) A public body shall, for the purposes of subsection (4), ensure that the data subject—

(a) has granted consent consciously and in a clear manner;

(b) may retrieve the content of the consent at any time; and

(c) may revoke the consent at any time with effect for the future.

**13.** (1) A public body may keep its records in electronic form.

(2) A public body shall ensure that where records are kept in electronic form, appropriate technical and organisational measures are implemented in accordance with accepted technological standards to ensure that the principles of orderly record-keeping and legal requirements for duration of maintenance of records are observed.

Electronic  
record-  
keeping

**14.** (1) Where a public body keeps electronic records, it shall keep electronic copies of those records on file in electronic form and may in accordance with this Act or any other law, retain paper documents.

Conversion  
and  
destruction  
of original  
paper  
documents

(2) A public body shall when transferring records to electronic documents, ensure that in accordance with accepted technological standards at the time the pictorial and text content of the electronic documents correspond to the paper documents when they are rendered readable.

(3) The National Coordinator may, on the request of a public body, waive the conversion of paper documents into electronic documents where that conversion would entail disproportionate technical efforts.

	(4) Subject to any other written law, a paper document may, following conversion into an electronic document, be archived, returned or destroyed as soon as further retention by the public body is no longer necessary on legal grounds or to ensure due quality of the conversion process.	5
Access to files	<b>15.</b> A public body shall, where a right to inspect a file exists, grant access to files by— (a) providing a print-out of the documents concerned; (b) displaying the electronic documents on a screen; (c) transmitting electronic documents; or (d) permitting electronic access to the content of the files.	10
Optimisation of administrative procedures and information on status of progress	<b>16.</b> (1) A public body may before introducing an information and communications technology system, apply established methods to document, analyse and optimise administrative procedures. (2) A public body shall, in the interests of the parties involved in the procedures, design the necessary work flows so that information on the status of progress and on the further course of the process can be retrieved by electronic means, together with contact information regarding the competent point of contact at the time of the inquiry concerned. (3) The National Coordinator may, on the request of a public body, waive the measures under subsection (1), where the measures will result in unreasonable costs or Joint automated procedures where those measures are impracticable or contrary to the purpose of the procedure concerned or breach a protective rule of law. (4) The processes under subsections (1) and (2) shall be documented. (5) Subsections (1) and (2) shall apply with necessary modification to any substantial changes to the administrative procedures or the information and communications systems used.	15 20 25 30
Joint automated procedures	<b>17.</b> (1) A public body may implement joint automated procedures with other public bodies to enable several data controllers to process personal data 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 information, be implemented in accordance with this Act and the Data Protection Act, 2021.	35
Act No. 3 of 2021		

(3) The participation of other public 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 bodies.

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

10 (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.

15 (5) The data controllers under subsection (1) shall appoint one of the participating public bodies whose data protection officer shall coordinate the implementation of this section by the participating public bodies.

20 (6) The data protection officer under subsection (5) shall cause to be prepared guidelines for coordination of joint automated procedure, which shall be available for inspection.

25 (7) Subject to the provisions of this Act, the Data Protection Act, 2021, Cyber Crime and Cyber Security Act, 2021 and any other relevant written law, a public body may commission another body to collect, process and use personal data for the joint automated procedure.

Act No. 3 of 2021  
Act No. 2 of 2021

(8) A data subject may assert that data subject's rights under the Data Protection Act, 2021, against any of the participating bodies, irrespective of which body is responsible for processing the data in the individual case concerned.

Act No. 3 of 2021

30 (9) A public body contacted by a data subject under subsection (8), shall forward the matter to a responsible public body in the case concerned.

35 **18.** (1) Where a public body employs publicly accessible networks to make data available, that public body shall use a machine-readable format as a general principle.

Requirements pertaining to provision of data

(2) A format under subsection (1), is machine-readable when the contained data can be read and processed in automated mode by means of corresponding software.

- Act No. 3 of 2021 (3) Subject to the other provisions of this Act and the Data Protection Act, 2021, data provided under subsection (1) shall be provided with metadata.
- (4) The President may, on the recommendation of the Division, make Regulations for use of the data under this section including commercial and non-commercial use, conditions of use and exclusion of liabilities and warranties. 5
- (5) For the purposes of this section “metadata” means a set of data that gives information about other data.
- Electronic forms 19. Where a legal provision stipulates the use of a form providing a signature field, the signature field may be omitted from a version of the form intended for electronic submission to the public body where an e-signature is used. 10
- Data protection Act No. 3 of 2021 20. (1) A public body shall implement data protection measures in accordance with the Data Protection Act, 2021. 15
- Act No. 3 of 2021 (2) Data protection under this Act shall be enforced in accordance with the Data Protection Act, 2021.
- Identity and authenticity 21. A data controller may only grant a right of access to personal data in which there is a protected interest in confidentiality within the meaning of Data Restriction on use of personal information Act No. 3 of 2021 Protection Act, 2021 in the context of electronic communications in the public sector, where the unique identity of the person desiring access and the authenticity of that person’s request is validated. 20
- Act No. 3 of 2021 (2) The validation under subsection (1) shall be provided in a form which can be verified electronically. 25
- (3) A data controller shall, where only recurring identity can be validated, grant access only in respect of personal data which the person requesting access has made available using that same identity. 30
- (4) The identification of a person may be requested in communications with a data controller by a public body, where it is an essential requirement for performance of a task assigned to that data controller under any law.
- Restriction on use of personal information Act No. 3 of 2021 22. A public body shall, without prejudice to the Data Protection Act, 2021, ensure that personal data is— 35
- (a) kept and used only for specified and lawful purposes for which the data is collected and processed; and
- (b) not kept for longer than is necessary for the purposes for which the data is collected and processed or as required by any law. 40

23. A public body shall not without lawful authority disclose information provided to that public body for the purpose or during the course of delivery of e-government services. Non-disclosure of information provided to public body
- (2) A person who contravenes subsection (1) commits an offence and is liable, on conviction —
- 5 (a) to a fine not exceeding two hundred thousand penalty units;
- (b) in the case of a second or subsequent offence, to a fine not exceeding five hundred thousand penalty units; and
- 10 (c) in the case of a continuing offence, to a fine not exceeding fifty thousand penalty units for each day on which the offence continues.
24. (1) A citizen card shall validate the unique identity of a person making a submission and of the authenticity of a submission made electronically in procedures for which a data controller in a public body has set up a technical environment in which the citizen card can be used. Citizen card
- 15 (2) A unique identification of a natural person who is the lawful holder of a citizen card shall be effected in that person's citizen card by way of an identity link and the ministry responsible for national registration shall confirm, by electronic signature, that
- 20 the natural person identified as the holder in the citizen card is allocated a particular source identification number for the purposes of unique identification.
- (3) An identity link shall be entered in the citizen card by the Ministry responsible for national registration or, on its behalf, by other public bodies, as prescribed.
- 25 (4) Authenticity of a submission made using a citizen card shall be validated by the electronic signature contained in that citizen card.
- 30 (5) A person who is not required to be registered in a public register shall, on application by that person at the request of a data controller, be registered by the Ministry responsible for national registration for the purposes of electronic validation of that person's unique identity.
- 35 (6) A source identification number shall, to the extent that it does not contain public data, be kept confidential subject to special protection by way of regulatory and technical measures of the citizen card scheme.

## PART V

## INFORMATION SYSTEMS SECURITY

- Information security **25.** The Division shall establish the Public Key Infrastructure for public bodies.
- Security of information **26.** A public body shall, in accordance with information security standards issued by the Division—
- (a) develop and enforce security measures to safeguard information collected or used in connection with e-government services from unauthorised disclosure; and
  - (b) take reasonable steps to ensure that every officer of the public body concerned with delivering services or collecting, placing, positing or disseminating information or services is aware of and complies with the security measures regarding the management and protection of information.
- Access to and sharing information Act No. 3 of 2021 **27.** (1) Subject to this Act, a public body may in the provision of Government services share with a private body information in accordance with the Data Protection Act, 2021.
- (2) The access to information shall be in accordance with the user rights and access levels as prescribed.
- Audit of public body **28.** (1) The Division may cause audits of a public body to be performed to evaluate compliance with the provisions of this Part.
- (2) An audit under subsection (1) may be performed by an inspector or an independent auditor.
- (3) The Division shall, where an audit reveals that a public body has contravened any provision of this Act, notify the public body in writing, stating the—
- (a) finding of the audit report;
  - (b) action required to remedy the non-compliance; and
  - (c) period within which a public body shall take the remedial action.

PART VI  
PUBLIC SERVICE ELECTRONIC TRANSACTIONS

29. (1) A public body which, 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, may—

Electronic filing, electronic signature and issuing of documents by public body

- (a) accept the filing of documents in electronic form;
- (b) issue a permit, licence or approval in electronic form; or
- (c) make or receive payment in electronic form.

10 (2) The Division may in relation to a public body that performs a function under subsection (1), specify by *Gazette* notice—

- (a) the manner and format in which the electronic communication shall be filed, created, retained or issued;
- (b) in cases where the electronic communication has to be signed, the type of electronic signature required;
- 15 (c) the manner and format in which an electronic signature may be attached or associated with the electronic communication;
- (d) the appropriate control processes and procedures to ensure adequate integrity, security and confidentiality of electronic communication or payments; and
- 20 (e) any other requirements for electronic communications or payments.

(3) A public body may adopt additional authentication procedures including the use of electronic notarisation systems or certificates of authentication on printed or hard copies of the electronic document or electronic data messages by electronic notaries, service providers and other duly recognised or appointed certification authorities.

30 30. (1) A public body may, where it consents to receive any information in electronic form, specify—

Receipt of information by public body

- (a) the manner and format in which the information shall be communicated to it;
- (b) the type or method of electronic signature required, if any;
- 35 (c) control processes and procedures to ensure integrity, security and confidentiality of the information; and
- (d) any other attributes for the information that is currently specified for corresponding information on paper.

(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 body otherwise than as specified or required by that public body.

Determination of originality of data message Act No. 4 of 2021

**31.** A public body shall, for the purposes of determination of 5 the originality of a data message under the Electronic Communications and Transactions Act, 2021, ensure that the integrity of any information shall be assessed—

(a) by considering whether the information has remained complete and unaltered, except for the addition of any 10 endorsement and any change which arises in the normal course of communication, storage and display;

(b) in relation to the purpose for which the information was generated; and

(c) having regard to all other relevant circumstances. 15

Use and acceptance of electronic signature for public body Act No. 4 of 2021

**32.** A public body may use and accept electronic signatures in accordance with this Act, Electronic Communications and Transactions Act, 2021 or any other written law.

Electronic Gazette

**33.** (1) The Government Printer may for the purposes of this Act, establish and maintain an electronic *Gazette*. 20

(2) Where any law provides that any rule, regulation, order, by-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, by-law, notification or any other matter is published in the *Gazette* or *e-Gazette*, except that, 25 where any rule, regulation, order, by-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.

(3) The Division may, for the purposes of subsections (1) and 30 (2), approve a website on which the information in the database may be published and accessed.

PART VII  
GENERAL PROVISIONS

34. As soon as practicable, but not later than ninety days after the end of the financial year, the Division shall submit to the President  
5 a report concerning its activities during the financial year. Annual reports

35. (1) The Surveyor-General shall, if an electronic document which contains information relating to real estate within the Republic is created or revised, include standard nationwide geo-referencing in the document relating to the respective parcel or the building or  
10 an area defined in a legal provision to which the information refers. Geo-referencing

(2) For the purposes of this Act, a document is one in respect of which data is collected or stored on the basis of legislation, which may be public or non-public documents.

36. (1) A person shall not without the consent in writing given  
15 by, or on behalf of the Division, publish or disclose 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. Prohibition of disclosure of information to unauthorised persons

20 (2) A person who contravenes subsection (1), commits an offence and is liable, on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding two years, or to both.

(3) Where a person having information which to such person's  
25 knowledge has been published or disclosed in contravention of subsection (1), unlawfully publishes or communicates such information to any other person, that person commits an offence and is liable, on conviction, to a fine not exceeding two hundred thousand penalty units or to imprisonment for a term not exceeding  
30 two years, or to both.

37. (1) The President may, by statutory instrument, make  
Regulations for the better carrying out of the provisions of this Act. Regulations

(2) Regulations made under this Act may empower a Minister that may be specified in the Regulations.

