GOVERNMENT OF ZAMBIA

STATUTORY INSTRUMENT No. 43 of 2023

The Electronic Government Act, 2021
(Act No. 41 of 2021)

The Electronic Government (General) Regulations 2023

IN EXERCISE of the powers contained in section 37 of the Electronic Government Act, 2021, the following Regulations are made:

1. These Regulations may be cited as the Electronic Government (General) Regulations, 2023. Title

2. In these Regulations, unless the context otherwise requires— Interpretation

"access" has the meaning assigned to the word in the Electronic Communications and Transactions Act, 2021; Act No. 4 of 2021

"data" has the meaning assigned to the word in the Electronic Communications and Transactions Act, 2021; Act No. 4 of 2021

"Data Protection Commissioner" has the meaning assigned to the words in the Data Protection Act, 2021; Act No. 3 of 2021

"digital platform" means a digital system and interface that facilitate communications, transactions and service delivery through digital channels;

"Division" has the meaning assigned to the word in the Act;

"electronic accessibility" means the process of making a digital product accessible to a consumer;

"e-government service" has the meaning assigned to the words in the Act;

Copies of this Statutory Instrument can be obtained from the Government Printer, P.O. Box 30136, 10101 Lusaka. Price K12.00 each.

"Government Service Bus" means an interoperable digital platform used by Government to provide electronic services;

"Government Wide Area Network" means a Government network that digitally connects public bodies within the Republic;

"incident" means an unplanned disturbance or effects of information technology services that result in a reduction in quality of service;

"marginalised group" means a vulnerable population or people that experience discrimination or exclusion to the use of information and communication technologies;

"paperless Government" means a Government that has minimal paper based processes and mainly relies on digitalised processes for its operations;

Act No. 3 of 2021

"processing" has the meaning assigned to the word in the Data Protection Act, 2021, and the word "processed" shall be construed accordingly;

Act No. 1 of 2018

"public body" has the meaning assigned to the words in the Public Finance Management Act, 2018; and

"vulnerability" means a flaw in a computer system that may be exploied by a security threat.

Notification of incident or vulnerability

3. A public body shall notify the Division, in the Form set out in the Schedule, of an incident or vulnerability that may affect e-government services immediately the incident or vulnerability is identified.

Electronic accessibility

4. A public body shall, for the effective delivery of e-government services —

(a) ensure that electronic services offered by that public body have electronic accessibility features for persons with disabilities;

(b) maintain and promote integrated and interoperable systems in the provision of services;

(c) ensure e-government services delivered have adequate support systems of end users; and

(d) ensure e-government services are delivered to marginalised groups.

Electronic record keeping

5. (1) A public body may store a record or document which is processed by that public body in an electronic format if the—

(a) information contained in that record remains accessible to be used for a subsequent reference;

(b) electronic record or document is retained in the format which represents accurately the information originally generated, sent or received; and

(c) details which facilitate the identification of the origin, destination, date and time of dispatch or receipt of that electronic record or document are available in electronic format.

Use of data by public body Act No. 3 of 2021

6. A public body shall use and process personal data in accordance with the Data Protection Act, 2021.

Security of data and digital platforms in public body

7. A public body shall—

(a) put security measures in place to ensure the security of data and its digital platforms;

(b) prepare and submit annual security reports to the Division in a form determined by the Division relating to its data and digital platforms; and

(c) conduct regular information and communication technology security risk assessments at such intervals as the Division may determine.

Localisation of personal data by public body

8. A public body shall store personal data processed by that public body on infrastructure domiciled within the Republic.

(2) Despite subregulation (1), a public body that intends to store personal data outside the Republic shall —

(a) obtain authorisation from the Division and the Data Protection Commissioner; and

(b) store personal data on terms and conditions that the Division and the Data Protection Commissioner may determine.

Integration with Government Service Bus

9. A public body shall—

(a) integrate its services with the Government Service Bus; and

(b) where applicable, provide its e-government services using the Government Wide Area Network.

Access to and sharing of information

10. (1) The Division shall, in collaboration with relevant institutions, determine the manner of access to, and sharing of, electronic information in a public body.

(2) A public body shall—

(a) ensure confidentiality, integrity and availability of data in the sharing of information; and

(b) develop an institutional policy on access to, and sharing of, information sharing.

Attainment of paperless Government

11. (1) A public body shall, within a period that the Division may determine, automate paper based processes and approvals of its operations.

(2) A public body shall, for purposes of attaining paperless Government—

(a) implement approved information and communication technology systems to digitise a public body's core processes; and

(b) ensure the implemented information and communication technology systems are interoperable to facilitate exchange of information within and among public bodies electronically.

Information and communication technology infrastructure

12. A public body shall use information and communication technology infrastructure that meets the specifications and standards set by the Division.

Information and communication technology asset register

13. A public body shall mantain and submit an information and communication technology asset register to the Division in a manner determined by the Division.

Audit and inspection by Division

14. (1) The Division shall conduct audits, quality assurance and inspection of electronic services provided by a public body as and when the Division considers necessary.

(2) A public body shall, for the purposes of compliance and audit, perform regular independent assessments and audits of its electronic and digital operations.

Information to be provided to Division

15. The Division may request a public body to provide, within a period that the Division may determine, documents and other information as the Division may require for the better carring out of its functions.

Information and communication technology education and utilisation

16. A public body shall, in collaboration with the Division, provide information and communication technology education and utilisation of e-government servces to the public relating to that public body.

SCHEDULE

FORM
(*Regulation* 3)

Republic of Zambia

The Electronic Government Act, 2021
(Act No. 41 of 2021)

The Electronic Government (General) Regulations, 2023

ELECTRONIC GOVERNMENT DIVISION INCIDENT AND VULNERABILITY REPORTING FORM

Name of public body
Nature of incident or vulnerability identified
Place of occurrence
What led to the incident?
Was there any harm to the information system?
What remedial actions will be taken to exclude future repetition of the incident?
Additional information on the incident or vulnerability
Comments from the Director/Head-Information and Communication Technologies in the institution
..... *Name of Permanent Secretary Head of institution* ..... *Signature*
Date: .....

LUSAKA
4th October, 2023
[SZI/64/9/4]

HAKAINDE HICHILEMA,
President