ARRANGEMENT OF SECTIONS

Section

1. Title.
2. Interpretation.
3. Processing of data.
4. Licensing of data controllers.
5. Validity and renewal of data controller licence.
6. Licence categories.
7. Submission of false information.
8. Exemption from licensing.
9. Register of licensed data controllers.
10. Obligations of data controller.
11. Sensitisation, educational awareness and training.
12. Appointment of data protection officers.
13. Guidelines on qualifications of data protection officers.
14. Functions of data protection officers.
15. Approval of codes.
16. Security of data.
17. Security breach notification.

FIRST SCHEDULE: Data Controller Application/Renewal Form DP1.

SECOND SCHEDULE: Fees.

THIRD SCHEDULE: DPO Designation/Appointment Notification .. Form DP2

FOURTH SCHEDULE: Breach Notification Form DP3.

IT is hereby notified that the Minister of Information Communications Technology, Postal and Courier Services in consultation with the Authority has, in terms of section 32 of the Cyber and Data Protection Act [*Chapter 12:07*], made the following regulations:—

Title

1. These regulations may be cited as the Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations, 2024.

Interpretation

2. In these regulations—

"Act" means Cyber and Data Protection Act [*Chapter 12:07*];

"Authority" means Data Protection Authority;

"biometric data" means physiological characteristics which are related to a data subject and include but are not limited to the following—

(a) fingerprints;

(b) palm veins;

(c) face recognition;

"DPO" means Data Protection Officer.

Processing of data

3. (1) No person shall process personal information for the purposes indicated in subsection (2) unless they are licensed with the Authority.

(2) Subject to section 4, any person who processes personal information with the intention to—

(a) decide the means, purpose or outcome of the processing;

(b) decide what personal data should be collected;

(c) decide which individuals to collect personal data from;

(d) obtain a commercial gain or other benefit from the processing of personal data;

shall apply for a licence in terms of these regulations.

(3) Any person who processes personal information in terms of this section without a data controller licence within the stipulated time frames shall be guilty of an offence and liable to a fine not exceeding level 11 or to imprisonment for a period not exceeding seven years or to both such fine and such imprisonment.

Licensing of data controllers

4. (1) Any person whether alone or jointly with others, who determines the purposes and means of the processing of personal data shall apply for a data controller licence.

(2) Any person who is required to apply for a data controller licence shall submit a written application in Form DP1 (Application/ Renewal Form) specified in the First Schedule to the Authority accompanied by a fee specified in the Second Schedule.

(3) The Authority shall after receiving an application referred to in subsection (2) —

(a) request for further information or supporting documents where necessary; or

(b) issue a data controller licence to a successful applicant; or

(c) reject an application for a data controller licence and give reasons;

within 14 days.

(4) The Authority may issue a data controller licence with such conditions as it may specify.

(5) Persons that are controlling data by the date of promulgation of these regulations shall submit their applications for a data controller licence within 6 months from the date of promulgation of these regulations.

(6) Any person who continues to process data without a license after the 6 months period provided for in subsection (5) shall be guilty of an offence and to liable to a fine not exceeding level 11 or to imprisonment for a period not exceeding seven years or to both such fine and such imprisonment.

Validity and renewal of data controller licence

5. (1) A data controller licence shall be valid for a period of 12 months subject to compliance with the Act, these regulations and licence conditions.

(2) A licensee may apply for renewal of the data controller licence using Form DP1 (Application/Renewal Form) specified in the

First Schedule, subject to a payment of a fee specified in the Second Schedule at least 3 months before the date of expiry of the licence.

(3) Any person who fails without just cause to renew their licence by the date of expiration of the previous licence, shall be guilty of an offence and liable to a fine not exceeding level 11 or to imprisonment for a period not exceeding 7 years or to both such fine and such imprisonment.

Licence categories

6. (1) The Authority shall issue any of the following data controller licences to any person eligible for licensing in terms of section 3—

(a) a tier 1 data controller licence shall be issued to a person who processes information for a minimum of 50 or a maximum of 1000 data subjects;

(b) a tier 2 data controller licence shall be issued to a person who processes information for a minimum of 1001 or a maximum of 100,000 data subjects;

(c) a tier 3 data controller licence shall be issued to a person who processes information for a minimum of 100,001 or a maximum of 500,000 data subjects;

(d) a tier 4 data controller licence shall be issued to a person who processes information for more than 500,000 data subjects.

(2) Any person who seeks to get a data controller licence in terms of subsection (1) shall on being issued with a licence, pay a licence fee specified in the Second Schedule.

Submission of false information

7. Any person who in the process of applying for a licence submits false information to the Authority shall be guilty of an offence and liable to a fine not exceeding level 11 or to imprisonment for a period not exceeding seven years or to both such fine and such imprisonment.

Exemption from licensing

8. (1) Data controllers processing personal data for one or more of the following purposes—

(a) personal, family or household affairs;

(b) law enforcement;

(c) journalistic, historical or archival purposes;

shall be exempted from applying for a data controller licence.

(2) A data controller referred to in subparagraph 1(b) and (c) shall be required to register with the Authority, and to comply with data protection principles under the Act.

Register of licensed data controllers

9. (1) The Authority shall maintain a register of all licensed and registered data controllers.

(2) Any person wishing to inspect the register of licensees and registered data controllers shall be free to do so at the Authority's premises or on the Authority's website.

Obligations of data controllers

10. (1)A data controller shall provide continuous professional development training to the data protection officer for purposes of maintaining the DPO certification.

(2) A data controller shall notify the Authority of the following—

(a) all processing activities performed on personal information;

(b) any modification of personal information collected indirectly from data subjects;

(c) any intention to transfer or share information of data subject outside Zimbabwe;

(d) any processing which involves biometric and genetic data of data subjects.

(3) A data controller shall not subject a data subject to a decision based solely on automated processing which produces legal effects concerning him or her without the consent of that data subject or based on a provision established by law.

(4) A data controller shall—

(a) be accountable for his or her representative, agent or assignee, data processor, recipient, data protection officer who contravenes the provisions of these regulations and the Act;

(b) take all the appropriate technical and organisational measures to safeguard the security, integrity and confidentiality of personal information which must ensure an appropriate level of security;

(c) be responsible for taking all the necessary measures and controls to comply with the principles and obligations set out in these regulations and the Act;

(d) put measures in place to facilitate the exercise of rights of data subjects under the Act;

(e) process personal information of physically, mentally or legally incapacitated data subjects through a parent or guardian or as provided for by the law or as directed by a court of competent jurisdiction;

(f) enter into a written data processing agreement or contract or legal instrument with a data processor which ensures that a data processor maintains all necessary security measures to safeguard personal information of data subjects.

(5) A data controller shall take into consideration the following when processing children's information—

(a) children's personal information shall not be processed without the consent of the parent or legal guardian of the child involved;

(b) any data controller processing personal information of children shall make reasonable efforts to verify that consent is given or authorised by the parent or legal guardian of the child, taking into consideration available technology;

(c) any controller processing children's data shall pay attention to all the data processing principles;

(d) any data controller processing children's data shall conduct regular data protection impact assessments to identify and mitigate privacy risks to children;

(e) any data controller must ensure data protection by design and data protection by default when processing children's data;

(f) no data controller shall subject children's data to automated decision making that has the effect of affecting the children's rights.

(6) Any data controller who contravenes this section shall be guilty of an offence and liable to a fine not exceeding level 11 or to imprisonment for a period not exceeding seven years or to both such fine and such imprisonment.

Sensitisation, educational awareness and training

11. (1) The Authority may provide public awareness sensitisation and trainings to data controllers, data protection officers and data subjects on data protection issues.

(2) The Authority shall provide certification training of data protection officers in conjunction with an institution of higher learning established in accordance with the laws of Zimbabwe or accredited institutions to provide such training after payment of fees specified in the Second Schedule.

(3) No person shall provide certification training for purposes of these regulations, unless the person is accredited by the Authority and has paid the fees set out in the Second Schedule.

(4) Any person who contravenes subsection (3) shall be guilty of an offence and liable to a fine not exceeding level 11 or to imprisonment for a period not exceeding seven years or to both such fine and such imprisonment.

Appointment of data protection officers

12. (1) A data controller shall appoint a data protection officer and notify the Authority in writing.

(2) The notice referred to in subsection (1) shall be in form DP2 specified in the Third Schedule.

(3) A data controller must notify the Authority of any change of the data protection officer's number, email address and physical address within a period of 14 days of such change.

(4) A data controller must notify the Authority of the dismissal or resignation of a DPO in writing within 14 days of termination of the DPO's contract.

(5) A data controller shall appoint a DPO within 90 days from the date of promulgation of these regulations or date of termination of the DPO contract.

(6) A data controller who fails to appoint a data protection officer in terms of subsection (1) shall be guilty of an offence and liable to fine not exceeding level 7 or to imprisonment not exceeding two years or to both such fine and such imprisonment.

Guidelines on qualifications of data protection officers

13. (1) A data protection officer shall have skill, qualifications, or experience in any of the following—

(a) data science; or

(b) data analytics; or

(c) information security systems; or

(d) information systems audit; or

(e) law; or

(f) audit; or

(g) any other relevant qualification;

(h) knowledge of national data protection laws and practices; and

(i) an understanding of the data controller's business operations and processing activities.

(2) Every data protection officer shall be required to undergo a certification course approved by the Authority.

(3) No person shall provide certification training for purposes of the Act and these Regulations, unless the person is accredited by the Authority and has paid the fees set out in the Second Schedule.

Functions of data protection officers

14. The duties of a data protection officer shall include—

(a) monitoring compliance with the Act and these regulations, and with organisational data protection polices, including—

(i) managing internal data protection activities;

(ii) raising awareness on data protection;

(iii) training staff on data protection; and

(iv) conducting internal data protection compliance audits;

(b) dealing with requests made to the data controller by the Authority and data subjects pursuant to the Act;

(c) advising employees about their obligations to comply with the Act and these regulations;

(d) advising on and monitoring of data protection impact assessments;

(e) working with the Authority in relation to the performance of its functions in relation to the data controller;

(f) act as the contact point of data subjects regarding the processing of their data.

Approval of codes of conduct

15. (1) Codes of Conduct shall be filed with the Authority for approval in terms of section 30 of the Act.

(2) In considering codes of conduct for approval, the Authority shall ascertain the following—

(a) whether the code complies with the Act;

(b) the level of representation of controllers or processors covered by the code of conduct;

(c) the inclusion of a concise statement explaining the purpose of the code, the benefits to members and how it effectively applies to the Act;

(d) identification of the processing operations that the code of conduct covers and the categories of controllers or processors that it applies to as well as the data protection issues that it intends to address;

(e) whether the code of conduct identifies suitable monitoring methods to assess member compliance with the code;

(f) complies with other relevant national legislation, where required.

(3) The Authority may seek the views of affected data subjects, or their representatives before approval of the code.

(4) The Authority may approve the code of conduct with or without amendments.

(5) Where the code owner seeks an amendment or review of the approved code, the processes outlined in subsection (2) shall apply.

(6) The Authority shall maintain a register of all approved codes of conduct.

Security of data

16. (1) Subject to section 18 of the Act, personal data shall be processed securely by means of appropriate technical and organisational measures.

(2) Technical and organisational measures include the following—

(a) conducting risk assessments;

(b) development and implementation of organisational policies;

(c) implementation of appropriate physical and technical measures shall apply to all data phases;

(d) controllers and processors may put in place additional measures about the security of processing depending on the circumstances and risk posed by the processing.

(3) The measures shall ensure the security, confidentiality, integrity and availability of the controllers' systems and services and the personal data being processed.

(4) The measures shall also enable the data controller or data processor to restore access and availability of personal data, in a timely manner in the event of a physical or technical incident.

(5) The data controller or data processor shall ensure that there are appropriate processes in place to test the effectiveness of the security measures, and to undertake any required improvements.

(6) The Cyber Security and Monitoring of Interception of Communications Centre and the Cyber Incident Response Team (zw-CIRT) may give technical advice to data processors and data controllers on security measures appropriate for specific controllers or categories of controllers.

(7) Any person who contravenes the provisions of this section shall be guilty of an offence and liable to a fine not exceeding level 11 or to imprisonment for a period not exceeding 7 years or to both such fine and such imprisonment.

Security breach notification

17. (1) A data controller shall report personal data breaches to the Authority within 24 hours of becoming aware of the breach affecting the data being processed by the concerned data controller or data processor.

(2) Personal data breaches shall be reported to the Authority by completing and submitting a data breach notification form DP3 (Data Breach Notification Form) specified in the Fourth Schedule.

(3) Where the detected breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the controller shall also inform those data subjects within 72 hours.

(4) A data controller shall—

(a) ensure that there are robust breach detection, investigation, and internal reporting procedures in place;

(b) keep a record of all personal data breaches.

(5) The data controller shall—

(a) cooperate with the Authority in conducting enquiries or investigations relating to data breaches;

(b) respond to information request on data breaches within 14 days; and

(c) conclude the data breach investigations and submit a report within 21 days from the date of notification.

(6) Any person who contravenes the provisions of this section shall be guilty of an offence and liable to a fine not exceeding level 11 or to imprisonment for a period not exceeding 7 years or to both such fine and such imprisonment.

First Schedule (*Sections 4 and 5)*

DATA CONTROLLER APPLICATION/ RENEWAL FORM DP1

POTRAZ - DATA PROTECTION AUTHORITY
P.O. Box MP 843, Mt Pleasant
1110, Performance Close
Mt Pleasant Business Park
Harare
Tel: 0242-333032/48
08677333032

1. Application Type Date: .....

Application No: .....

Data Controller License No:.....

2. Data Controller Category

Tier 1 - minimum of 50 or a maximum of 1000 data subjects.

Tier 2 - minimum of 1001 or a maximum of 100,000 data subjects.

Tier 3 - minimum of 100,001 or a maximum of 500,000 data subjects.

Tier 4 - more than 500,000 data subjects.

3. Client Information

Applicant Name:.....

Certificate of Incorporation Number: .....

Physical Address: .....

Postal Address: .....

Telephone No: .....Cell No:.....

E-mail:.....

Scope of Business: .....Country: .....

Name of Designated DPO:.....

DPO Contact Email: .....

Tel No:.....

Cell No: .....

4. Type of Business (tick the applicable)

Crime Prevention / Law Enforcement
Financial Services
Education
Health Administration and Patient care
Hospitality
Property Management
Telecommunications
Entities processing Genetic Data
Political Parties
Media and Broadcasting
Government Department/Ministry
Consultants services
Construction & Civil engineering
Other (Specify) .....

Description of personal data being processed

5. Sensitive personal data collected and processed

Do you handle any sensitive personal data?

Yes

No

If yes, please complete the table below:

	Type of data	Purpose of processing
(a)	Racial or ethnic origin:	
(b)	Political opinions:	
(c)	Membership of a political association:	
(d)	Religious beliefs or affiliations:	
(e)	Philosophical beliefs:	
(f)	Membership of a professional or trade association:	
(g)	Membership of a trade union:	
(h)	Sex life:	
(i)	Criminal educational, financial or employment history:	
(j)	Gender, age, marital status or family status:	
(k)	Health/ biometric data:	

6. Data processing location

Is your data located in Zimbabwe?

Yes

No

If No, State the Country: .....

7. Data security

Explain the safeguards in place to protect the data?

Applicant's signature: .....Position held: .....Date: .....

Declaration by Applicant: .....

I,..... in my capacity as the representative of ..... who is the data controller hereby solemnly swear that the information contained in this form is to the best of my knowledge true and correct.

Thus, done and signed on behalf of.....
(Data controller) at .....on this..... day of ..... 20 .....

FOR OFFICE USE ONLY

Fee Class: .....Total Fee: .....Receipt No: .....

Recommending Officer: .....Date:.....

Approving Officer: .....Date:.....

Comment(s).....

.....

.....

SECOND SCHEDULE (*Sections 4,5,6 and 11*)

FEES

Data controller licence fees: Payable in USD or in ZiG at the official exchange rate.

1. Application fees for Tier 2, 3 or 4 licences USD 30

2. Initial/ Renewal fees

(i) Tier 1licence USD 50

(ii) Tier 2 licence USD 300

(iii) Tier 3 licence USD 500

(iv) Tier 4 licence USD 2 500

3. Training Accreditation fees USD 5000, *per annum*

4. DPO training and certification fees—

(i) Zimbabwean citizens USD 1 250, per person

(ii) International USD 1 450, per person

5. DPO training application fees—

(i) Zimbabwean citizens USD 30, per person

(ii) International USD50 per person

6. Ad hoc training fees: the Authority may charge fees for ad hoc training activities that it may conduct from time to time.

THIRD SCHEDULE (*Section 12*)

DPO DESIGNATION/APPOINTMENT NOTIFICATION FORM DP2

POTRAZ - DATA PROTECTION AUTHORITY

DPO DESIGNATION/APPOINTMENT NOTIFICATION FORM

POTRAZ - DATA PROTECTION AUTHORITY
P.O. Box MP 843, Mt Pleasant
1110, Performance Close,
Mt Pleasant Business Park,
Harare
Tel: 0242-333032/48
08677333032

1. Client Information

Name of Data Controller: .....

Data controller licence number: .....

Physical Address: .....

Postal Address: .....

Telephone No: .....Cell No: .....

E-mail address: .....

Scope of business operations:.....

Name of appointed data protection officer: .....

Data protection officer registration number: .....

Email of Data Protection Officer:.....

Tel No: .....

Cell No:.....

Address of data protection officer:

.....

.....

.....

.....

Educational and professional qualification:

.....

FOURTH SCHEDULE (*Section 17*)

BREACH NOTIFICATION FORM DP3

POTRAZ - DATA PROTECTION AUTHORITY
P.O. Box MP 843, Mt Pleasant
1110, Performance Close,
Mt Pleasant Business Park,
Harare
Tel: 0242-333032/48
08677333032

1. Client Information

Name of Controller:.....

Data Protection License Number: .....

Physical Address: .....

Postal Address: .....

Telephone No: ..... Cell No: .....

Name of designated data protection officer: .....
.....

Email address of data protection officer: .....

Tel No: .....

Cell No: .....

2. Scope of Breach

1. Date of data breach .....
2. Date of breach identification .....
3. Information systems breached .....

4. Nature of personal data affected, categories and approximate number of records affected.

5. Likely impact of the data breach

6. Measures taken or to be taken to address the data breach:
