Statutory Instrument ……. of 2022

[CAP. 12:07]

Cyber and Data Protection (Licensing of Data Controllers and Appointment of DPOs) Regulations, 2022 (No...)

IT is hereby notified that the Minister of Information and Communications Technologies has, in terms of section 32 of the Cyber and Data Protection Act [*Chapter 12:07*], made the following regulations after consultations with the Authority: -

1. These regulations may be cited as the Cyber and Data Protection Regulations, 2022 (No. …)
2. These regulations shall be deemed to come into operation on the date of publication.

PART I

3. Licensing and Registration of Data Controllers

(1) A person, entity or public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data shall apply for a data protection licence.
(2) Data controllers must carry out a self- assessment in terms of the licensing eligibility tool available at the Authority's website and Form DP1 contained in Part I of the First Schedule.
(3) Data Controllers eligible for licensing shall apply for data protection licence and renew registration annually using Form DP2 contained in Part II of the First Schedule.
(4) An applicant for data protection licence or a licensee shall pay an applicable application or renewal fee specified in the Second Schedule.
(5) The application for data protection licence shall be made within the months of these regulations coming into effect ,in the case of existing entities employing more than 30 persons or with a gross turnover of
(6) The Authority shall maintain a register of licensed data controllers.

4. Licence Categories
   (1) The Authority shall issue any of the following data protection licences to a data controller eligible for licensing in terms of section 3(1)-
   (a) Tier 1 Data Protection Licence
   A Tier 1 Data Protection licence shall be issued to organisations with a maximum of 50 employees or a minimum annual gross turnover of or exceeding. US$500 000 ,as the case may be
   (b) Tier 2 Data Protection Licence
   A Tier 2 Data Protection Licence shall be issued to small to medium enterprises or joint controllers with a minimum of 50 and a maximum of 75 employees or a minimum annual gross turnover of US$1,000,000.00

(c) A Tier 3 Data Protection Licence shall be issued to a large enterprise or joint controllers with a minimum of 76 employees, or a total annual gross turnover of more than US$1,000,000.00
(d) Special Data Protection Licence issued under section 5.

5. Special data protection licence

(1) Public authorities, statutory bodies and religious organisations shall apply for a special data protection licence in terms of this section upon payment of an application or renewal fee specified in the First Schedule.

6. Exemption from licensing

(1) Data controllers processing personal data for one or more of the following purposes:
I. Not-for-profit purposes.
II. Personal, family or household affairs.
III. Judicial functions.
shall be exempt from applying for a data protection licence.

(2) A data controller referred to in sub-paragraph (1) above shall be required to register with the Authority.
(3) The Authority shall maintain a register of all data controllers exempted from licensing.

PART II

Data Protection Officers

7. Designation of a data protection officer

(1) A data controller is required to appoint or designate a data protection officer for all unexempted purposes including where:
(a) the processing is carried out by a public authority or body.
(b) the core activities of the controller or the processor consist of data processing operations, which require regular and systematic monitoring of more than 3000 subjects: or
(c) the core activities of the controller or the processor consist of processing of special categories of data or personal data relating to criminal convictions and offences where the processing operations cover more than 1000 people;
(d) Data processing described in sub-paragraph (c) above excludes processing done for judicial functions or law enforcement purposes.
(2) Organisations should publish the details of their data protection officers on their websites, widely read newspapers or prominent notice boards.
(3) Organisations or data controllers should notify the Data Protection Authority of the designation or appointment of their data protection officer by completing an online form available on the Authority's website and submit via email or use Form DP3 contained in the III Schedule.

(4) A Data Controller must notify the Authority of the change of Data Protection Officer's contact details within a period of 14 days of such change.
(5) A Data Controller must notify the Authority of the dismissal or resignation of a DPO via email within 14 days of termination of DPO contract.
(6) A data controller shall appoint a DPO or re-appoint another DPO within 6 months from the promulgation of these Regulations or date of termination of contract of the incumbent DPO.

8. Guidelines on qualifications of data protection officers

(1) Relevant skills and expertise of data protection officers shall include but are not limited to:
   i. expertise in national data protection laws and practices including an in-depth understanding of the Cyber and Data Protection Act.
   ii. In-depth understanding of how their organisation processes personal data;
   iii. Understanding of information technologies and data security;
   iv. Thorough knowledge of their organisation and the business sector in which it operates;
   v. Ability to promote a data protection culture within the organisation.

(2) Every Data Protection Officer shall be required to undergo a certification course offered or approved by the Authority and offered by the Authority, or institutions appointed or designated by the Authority, as National Data Protection Training Institutions,within three months of the coming into effect of this regulations, or in the case Data Protection Officers appointed after the three months have lapsed, before assuming duty as a data protection officer
(3) Every Data Protection Officer shall undergo certification renewal once a year
(4) 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 2nd Schedule.

9. Functions of data protection officers

The Duties of a data protection officer shall include:
1) Ensuring compliance by the data controller with the provisions of the Act and these regulations.
2) Dealing with requests made to the data controller by the Authority pursuant to this Act.
3) Informing and advising the employees about their obligations to comply with the Act and other data protection laws.
4) Monitoring compliance with the Act and other data protection laws, and with organisational data protection polices, including managing internal data protection activities, raising awareness of data protection issues, training staff, and conducting internal audits.
5) Advising on and monitoring of data protection impact assessments.
6) Cooperating with the Authority.

7) Being the first point of contact for the Authority, and for individuals whose data is processed (employees, customers etc).

PART III
Requirements for Processing

10. Processing for Legitimate interests

1) subject to section 10 (4) of the Act, if a controller chooses to rely on legitimate interests for processing data, a Legitimate Interest Assessment (LIA) must be conducted first, and a record of such LIA should be kept properly to demonstrate compliance.
2) Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.
3) A data controller should satisfy the following key elements to the legitimate interests basis:
    a) identify a legitimate interest;
        i. legitimate interest can be organisational interests or interests of third parties,
        ii. these may include commercial interests, individual interests, or broader societal benefit.

    b) show that the processing is necessary to achieve the legitimate interests;
        i. the processing must be necessary, and
        ii. if the controller can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.
    c) balance legitimate interests against the individual's interests, rights and freedoms;
        i. if the data subject would not reasonably expect the processing, or
        ii. if processing would cause unjustified harm, the individual interests may override the controller's legitimate interests.
4. A data controller should include details of its legitimate interests in its privacy policy.

11. Processing of Health Data

1) Health Data should be processed lawfully.
No person shall be subjected to medical or scientific experiments or the extraction or use human tissue without the Informed consent of the data subject unless authorised by law.

2) Where processing without the consent of the data subject is necessary for the prevention of imminent danger or for the mitigation of a specific criminal offence, such processing shall only be carried out in terms of a court order, or an authorisation issued in terms of the Public Health Act [Chapter 15:17].

PART IV

Codes of Conduct and approval process

12. Codes of conduct

1) Codes of conduct are voluntary accountability tools which should help the controllers to comply with the CDPA,
2) The Code of conduct shall cover appropriate data protection processing elements applicable to specific data controllers or categories of data controllers such as lawful, fair, and transparent processing, legitimate interests, data retention, security etc.
3) Codes of conduct shall also reflect the specific needs of controllers and processors in small and medium enterprises and help them to work together to apply the CDPA requirements to specific issues that they face.
4) Codes should provide added value for their sector, as they will tailor the CDPA requirements to the sector or area of data processing.
5) Codes shall also provide for monitoring and compliance mechanisms for a sector and its members.
6) National codes of conduct may specify the circumstances and procedure for transfer of personal information outside Zimbabwe

13. Approval of Codes

1) Codes of Conduct shall be filed with the Authority for approval in terms of s30 of the CDPA.
2) In considering codes of conduct for approval, the Authority shall ascertain the following:
   a) Whether the code complies with the CDPA.
   b) The code owner's ability to represent controllers or processors covered by the code.
   c) The inclusion of a concise statement explaining the purpose of the code, the benefits to members and how it effectively applies the CDPA.
   d) Identification of the processing operations that the code 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 identifies suitable monitoring methods to assess code member compliance with the code.
   f) Outline of the stakeholder consultation and outcomes.
   g) Complies with other relevant national legislation, where required.

3) The Authority may seek the views of affected data subjects, or their representatives before approval.
4) The Authority may approve with or without amendments.
5) Where the code owner seeks an amendment of review of the approved code, the processes outlined in sub sections 2 shall be repeated.
6) The Authority shall maintain a register of all approved codes of conduct.

PART V

Security

14. Security of Data

1) subject to section 18 of the CDPA, personal data shall be processed securely by means of appropriate technical and organisational measures.
2) Technical and organisational measures entail the following:
   i. conducting of risk analysis.
   ii. development and implementation of organisational policies.
   iii. implementation of appropriate physical and technical measures such as pseudonymisation and encryption.
   iv. Controllers and processors should take into account additional requirements about the security of processing depending on the circumstances and risk posed by processing.
3) The measures must ensure the confidentiality, integrity and availability of the controller' systems and services and the personal data being processed.
4) The measures must also enable the controller or processor to restore access and availability to personal data, in a timely manner in the event of a physical or technical incident.
5) The controller or processor should 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 may in terms of section 4 of the Interception of Communications Act (as amended by Act 5 of 2021) give technical advice to data processors and controllers on security measures appropriate for specific controllers or categories of controllers.

15. Security Breach notification

1) A controller should report personal data breaches to the Authority within 24 hours of becoming aware of the breach affecting the data being processed by the concerned controller or processor.
2) Personal data breaches should be reported to the Authority by completing and submitting a Data Breach Notification Form DP4 contained 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 must also inform those individuals without undue delay.
4) A controller should ensure that there are robust breach detection, investigation, and internal reporting procedures in place.
5) A controller must keep a record of any personal data breaches.

FIRST SCHEDULE

PART I
Data Controller Self-Assessment FORM DP1

Instructions

- Please Complete ALL the Sections of the Assessment tool
- Both Data Controllers and Data Processor use the same self-assessment form
- Enter valid primary e-mail address

SECTION 1 – Data Controller and Processor Checklist

You are a DATA Controller if :

☐You decide to collect or process the Personal Data.
☐You decide what the purpose or outcome of the Processing will be.
☐You decide what Personal Data should be collected.
☐You decide which individuals to collect Personal Data from.
☐You obtain a commercial gain or other benefit from the Processing of Personal Data
☐You are Processing the Personal Data because of a contract between you and the Data Subject.
☐The Data Subjects are your employees.
☐You make decisions about the individuals concerned as part of or because of the Processing.
☐You exercise professional judgement in the Processing of the Personal Data.
☐You have a direct relationship with the Data Subjects.
☐ You have complete autonomy as to how the Personal Data is processed.
☐ You have appointed the processors to process the Personal Data on your behalf.

You are a Data Processor if:

☐You have a contract to handle Personal Data on behalf of another Entity.
☐ You are following instructions from someone else regarding the Processing of Personal Data.
☐ You do not decide to collect Personal Data from individuals.
☐ You do not decide what Personal Data should be collected from individuals.
☐ You do not decide the lawful basis for the use of that data.
☐ You do not decide what purpose or purposes the data will be used for.
☐ You do not decide whether to disclose the data, or to whom.
☐ You do not decide how long to retain the data.
☐ You may make some decisions on how data is processed but implement these decisions under a contract with another Entity.

SECTION 2: Entity Characteristics

Entity Characteristics

1) **Annual Turnover**

Is your annual turnover:

- (•) Less than USD500,000
- ( ) US $500,000 < Annual Revenue

2) **Staff Complement**

- **Less than 50**
- **Above 50**

Above 50

DATA CONTROLLER APPLICATION/RENEWAL LICENCE FEES

Payable in ZWL at the official exchange rate.

Tier 1licence	USD 500per annum
Tier 2 licence	USD 1000 per annum
Tier 3 licence	USD 2000 per annum.
Special Licence	USD 200 per annum
Training Accreditation fees	USD 5000 per annum

Training and certification fees

Tier 1	USD 100 per person
Tier 2	USD 300 per person
Tier 3	USD 500 per person

Data Privacy Assessments

Tier 1	USD 200 per day
Tier 2	USD 400 per day
Tier 3	USD 500 per day

Third Party due diligence checks

Tier 1 USD 500 per day
Tier 2 USD 1000 per day

- Tier 3 USD 3000 per day

(•) Less than 30

( ) Above 30

- Less than 50
- Above 75

3) Entity type

( ) Private Sector Entity

( ) Public Sector Entity

NB:

If your entity has selected item 1(b) or 2(b) or 3(b) , you must apply for a Data Controller Licence with the Authority.

PART II

Data Controller Application FORM DP2

POTRAZ - DATA PROTECTION AUTHORITY

P.O. Box MP 843, Mt Pleasant
1110 Performance Close
Mt Pleasant Business Park
Harare
Tel: 0242-333032
08677333032

DATA CONTROLLER APPLICATION FORM

1. Application Type

Date:……
Application No……
License No……...

- □ Data Controller
- □ Data Processor

2. Data Controller Category
(where "*x*" is the number of employees and "*y*" is annual gross turnover)

- □ Tier 1 ($x \geq 20$ *or* $y = ZWL$)
- □ Tier 2 ($21 \leq x \leq 50$ or $y \geq$ ZWL)
- □ Tier 3 ($51 \leq x$ *or* $y \geq ZWL$)
- □ Special Data Protection Licence issued under section 5.

3. Client Information

Applicant Name :……...

Certificate of Incorporation ……. ……..

Physical Address……..……

Postal Address……

Telephone/Cell No……..Fax No……...

E-mail…….

Scope of Business……..……Country …….…..

Name of Designated DPO (optional)……

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

5. Description of Personal Data Processing

6. 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;	

	Type of Data	Purpose of Processing
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;	

7. **Data Location**

Is your Data located in Zimbabwe ?

- ☐ Yes
- ☐ No

If No, State the Country ……

8. **Data Security**
   Explain the Safeguards in place to protect the data?

Applicant Signature……Position Held……Date……

FOR OFFICE USE ONLY

Fee Class…….. Total Fee…….Receipt No……

Recommending Tech Officer……..Approved Date……

Approving Officer……

Comment(s)…….……

…….……

…….……

SECOND SCHEDULE

DATA CONTROLLER APPLICATION/RENEWAL LICENCE FEES

Payable in USD or in ZWL at the official exchange rate.

Tier 1licence	USD 200 per annum
Tier 2 licence	USD 400 per annum
Tier 3 licence	USD 600 per annum.
Special Licence	USD 100 per annum
Training Accreditation fees	USD 5000 per annum

Training and certification fees

Tier 1	USD 200per person
Tier 2	USD 300 per person
Tier 3	USD 500 per person

Data Privacy Assessments

Tier 1	USD 100 per day
Tier 2	USD 300 per day
Tier 3	USD 500 per day

Third Party due diligence checks

Tier 1	USD 500 per day
Tier 2	USD 1000 per day
Tier 3	USD 3000 per day

THIRD SCHEDULE

DPO DESIGNATION/APPOINTMENT 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
08677333032

'creating a level playing field'

DPO DESIGNATION/APPOINTMENT NOTIFICATION FORM

1. Client Information

Name of Controller or Processor ……...

Data Protection License Number ……. ……..

Physical Address……..……

Postal Address……

Telephone/Cell No……..Fax No……...

E-mail…….

Scope of Business Operations

☐Data Processor
☐Data Controller

Name of Designated Data Protection Officer ……

Email of Data Protection Officer ……..

Tel #…….

Mobile #……...

Address of the Data Protection Officer :

……

……

……

……

'creating a level playing field'

FOURTH SCHEDULE

Breach Notification Form DP4

POTRAZ - DATA PROTECTION AUTHORITY

P.O. Box MP 843, Mt Pleasant
1110 Performance Close
Mt Pleasant Business Park
Harare
Tel: 0242-333032
08677333032

DATA BREACH NOTIFICATION FORM

9. Client Information

Name of Controller or Processor ……...

Data Protection License Number ……. ……..

Physical Address……..……

Postal Address……

Telephone/Cell No……..Fax No……...

Name of Designated Data Protection Officer ……

Email of Data Protection Officer ……..
Tel #…….

Mobile #…….....

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: