'creating a level playing field'

Data Protection Authority Implementation Guidelines on the Cyber and Data Protection Act [Chapter 12:07]



Guidelines Overview

These Implementation Guidelines have been developed by the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) in its capacity as the designated Data Protection Authority in terms of section 5 of the Cyber and Data Protection Act [Chapter 12:07] (CDPA). The CDPA in Section 6 (1) (a) requires the Authority to set the conditions for the lawful processing of data in Zimbabwe. These Guidelines seek to provide practical direction on the application, interpretation, and operationalisation of the CDPA and Statutory Instrument 155 of 2024. By translating legal provisions into clear implementation steps, these Guidelines aim to:

- enhance understanding,
- promote accountability and,
- strengthen a culture of data protection compliance.

These Guidelines will equip data controllers and data subjects with the necessary skills and knowledge to comply with the law.

Contents

1 Implementation Guidelines on Compliance Assessments **Page 4**

2 Implementation Guidelines on Continuous Professional Development Assessment for Certified Data Protection Officers **Page 17**

3 Implementation Guidelines on How to Conduct a Data Protection Impact Assesment (DPIA) **Page 23**

4 Implementation Guidelines for Adequate Level Of Protection Under Cross-Border Data Transfers **Page 32**

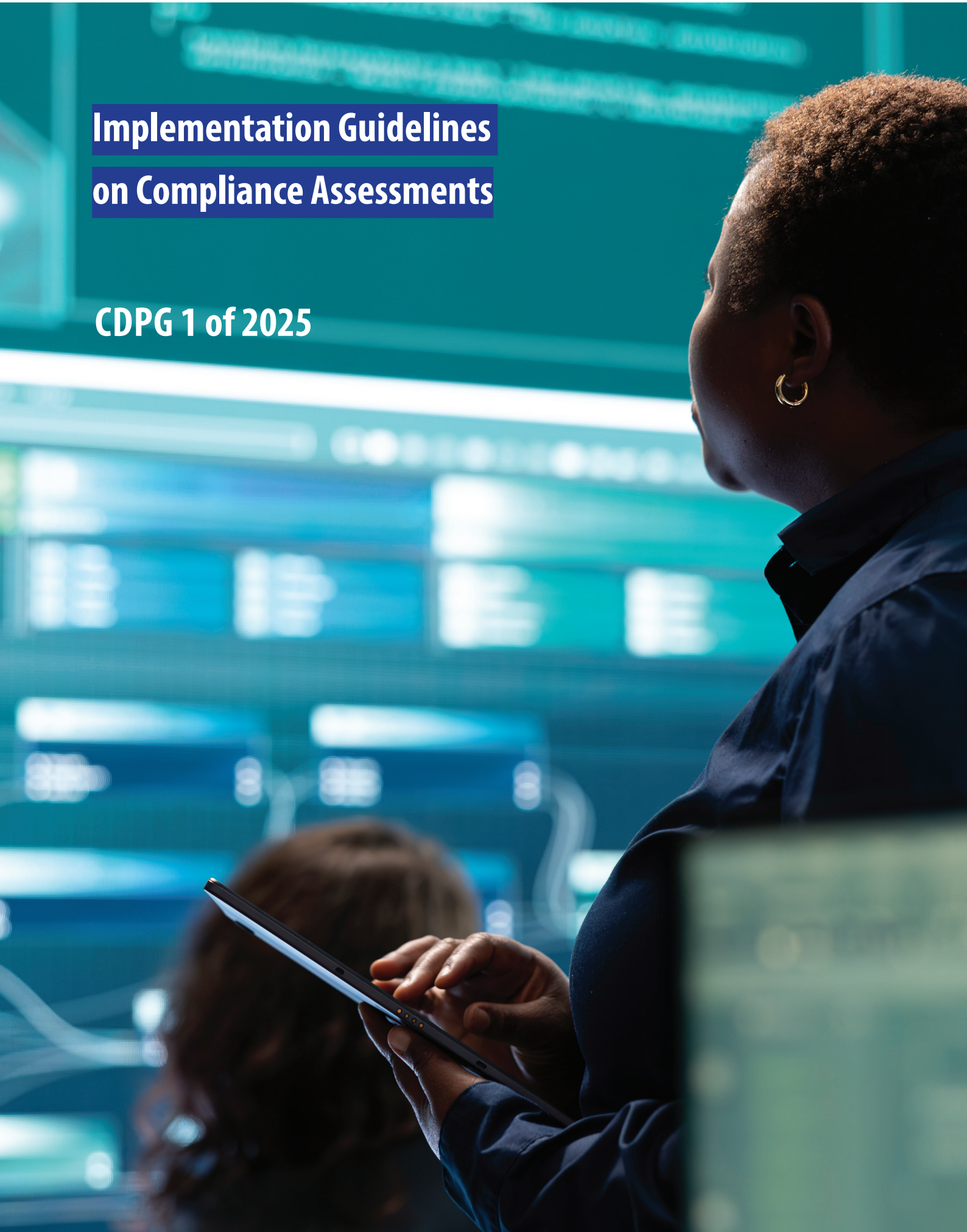
5 Guidelines on the Licensing of Government Ministries, Departments & Agencies (MDAS) **Page 36**

6 Implementation Guidelines: Processing of Personal Data by Political Parties, Independent Candidates and Electoral Stakeholders **Page 40**

7 Implementation Guidelines on the Processing of Personal Information by Micro-Small to Medium Enterprises (MSMEs), in Zimbabwe **Page 48**

Implementation Guidelines on Compliance Assessments

CDPG 1 of 2025



Implementation Guidelines on Compliance Assessments

1. INTRODUCTION

These guidelines establish the framework, standards, and procedures for compliance assessments to be carried out by the Data Protection Authority (DPA), hereinafter referred to as the Authority, in respect of data controllers operating under the Cyber and Data Protection Act [CDPA]. The purpose of these guidelines is to ensure that all data controllers subject to the Act are held to a consistent, transparent oversight process, thereby strengthening the culture of accountability and compliance in Zimbabwe's data protection landscape.

The guidelines are issued in terms of section 6(1)(a) of the Cyber and Data Protection Act, which empowers the Authority to regulate the manner in which personal information may be processed through the establishment of clear conditions for the lawful processing of data. In line with this mandate, these guidelines provide a structured approach for assessing whether data controllers have in place the necessary governance, technical, and organisational measures to comply with the law.

By issuing these guidelines, the Authority seeks to promote a consistent, fair, and transparent compliance assessment regime that not only enforces the law but also supports data controllers in building robust data protection practices. Ultimately, the objective is to ensure that the processing of personal information in Zimbabwe is conducted in a lawful, fair, and accountable manner, thereby safeguarding the rights and freedoms of data subjects while fostering trust in the digital economy.

2. OBJECTIVES OF COMPLIANCE ASSESSMENTS

The main objectives of the compliance assessment are:

1) Evaluate the level of compliance of data controllers with the CDPA and related regulations.
2) Identify and address gaps in data protection governance, policies, and practices.
3) Promote a culture of accountability and continuous improvement in personal data handling.
4) Provide recommendations for remedial action and risk mitigation.

3. TYPES OF COMPLIANCE ASSESSMENTS

In carrying out its mandate under the Cyber and Data Protection Act (CDPA), the Authority adopts a risk-based, proportionate, and transparent approach to compliance monitoring. The following types of compliance assessments may be conducted for data controllers to ensure compliance with the conditions for lawful processing of personal information.

3.1. Voluntary Assessment

A voluntary assessment is an evaluation initiated at the request of the data controller. In this instance, the data controller submits a written invitation to the Authority, indicating its willingness to undergo a compliance review. The invitation should include a proposed date and time for the assessment.

This type of assessment is collaborative, advisory, and non-punitive. It is not intended to result in the imposition of fines, sanctions, or corrective orders. Instead, it serves as a mechanism for data controllers to identify compliance gaps, strengthen their internal processes, and demonstrate commitment to lawful data processing practices. By taking the initiative, data controllers can proactively rectify deficiencies before they escalate into regulatory violations.

Procedure:

- The data controller submits a formal written request to the Authority, suggesting a proposed date and time for the assessment.
- The Authority reviews the request and confirms, in writing, an agreed-upon schedule.
- The assessment is conducted in accordance with an agreed methodology. The Authority, however, reserves the right to recommend or adopt an alternative method where necessary to achieve its regulatory objectives.
- Upon conclusion, the Authority provides advisory feedback highlighting areas of compliance and opportunities for improvement.

3.2. Routine Planned Assessment

A routine planned assessment is a scheduled evaluation conducted by the Authority as part of its annual compliance monitoring programme. These assessments are intended to promote a culture of sustained readiness among data controllers and ensure that compliance with the CDPA is embedded in day-to-day operations.

The Authority will provide the data controller with at least seven (7) days' written notice before the assessment. The notification will outline the scope of the evaluation, the methodology to be applied, and the preliminary documentation required. It will also specify the categories of records that may be reviewed and the key personnel who are expected to participate in interviews or discussions.

It must be noted that during a routine planned assessment, the Authority retains the right to request additional documentation, test relevant systems, or interview personnel not initially listed in the notification, where such measures are reasonably necessary to fulfil its mandate.

Procedure:

- The Authority issues a formal written notification to the data controller specifying the proposed date, scope, methodology, and preliminary information requirements.
- The data controller is provided sufficient time to prepare and to submit the requested documentation in advance of the assessment.
- The Authority conducts the assessment using the agreed framework but may expand its scope where necessary to ensure completeness and integrity of the evaluation.

3.3. Ad Hoc (Unannounced) Assessment

An ad hoc, or unannounced, assessment is conducted by the Authority without prior notice to the data controller. Such assessments are triggered by specific circumstances, including receipt of a complaint by a data subject, a data breach notification, intelligence suggesting non-compliance, or other factors that raise reasonable suspicion of unlawful processing.

The purpose of an ad hoc assessment is to enable the Authority to investigate urgent or high-risk compliance concerns in a timely and effective manner. The fact that such an assessment is carried out does not, in itself, imply that the data controller has committed a violation; rather, it reflects the Authority's obligation to verify compliance where risks have been identified. Data controllers should therefore ensure that they are in a state of readiness at all times to facilitate such inspections.

Procedure:

- The Authority's assessment team arrives at the premises of the data controller without prior scheduling or notification.
- Upon arrival, the team formally identifies itself and presents official authorisation to the accounting officer or the designated point of contact within the organisation.
- The assessment proceeds in accordance with the Authority's investigative powers under the CDPA, which may include document review, interviews, system checks, and on-site inspections.

3.4. Self-Assessment by Data Controllers

In addition to compliance assessments conducted by the Authority, a Data Controller may undertake a self-assessment to evaluate its own level of compliance with the Cyber and Data Protection Act and any subsidiary regulations or guidelines. The self-assessment shall be carried out using an approved self-assessment tool or online link provided by the Authority. This tool is designed to enable Data Controllers to identify compliance gaps, evaluate internal data protection controls, and measure progress in implementing the Act's requirements.

Alternatively, a Data Controller may engage the services of a Certified Data Protection Officer (DPO) or a data protection consultancy that is duly registered and authorised by the Authority to conduct compliance assessments on its behalf. Such engagements shall be voluntary and undertaken in accordance with the standards and methodologies prescribed by the Authority.

Upon completion of the self-assessment, the Data Controller shall prepare a Self-Assessment Report summarising the findings, identified gaps, and corrective measures to be implemented. This report shall be submitted to the Authority for verification and record-keeping. The Authority may, where necessary, conduct a follow-up review or verification assessment to confirm the accuracy of the self-assessment and the adequacy of remedial measures taken.

The purpose of this provision is to promote a culture of accountability and continuous improvement among Data Controllers.

These four categories of assessments, voluntary, routine planned, ad hoc and self-assessments, collectively provide the Authority with a comprehensive toolkit for monitoring compliance. They balance encouragement of proactive cooperation by data controllers with the need for regulatory vigilance to safeguard the rights of data subjects and uphold the principles of lawfulness, fairness, transparency and accountability in data processing.

4. ASSESSMENT METHODS

In fulfilling its compliance monitoring mandate, the Authority applies a range of assessment methods designed to ensure flexibility, proportionality, and effectiveness. The choice of method will depend on the nature of the assessment, the data controller's risk profile, and the circumstances giving rise to the review. The principal techniques are outlined below.

4.1. Onsite Assessment

An on-site assessment involves the Authority's officials visiting the data controller's premises to evaluate compliance with the Cyber and Data Protection Act directly. This method allows the Authority to observe processing operations in their actual environment, conduct face-to-face interviews with staff, and review relevant documents and systems.

During an on-site assessment, the Authority may also conduct inspections of physical and digital security measures and observe how data-handling practices align with stated policies. Where necessary, the Authority may record proceedings or take photographs as evidence, strictly for official use in preparing the compliance assessment report. This approach provides a comprehensive and holistic view of the data controller's operations.

4.2. Offsite Assessment

An off-site assessment is conducted at the Authority's offices, where the data controller is invited to attend for a compliance review. The Authority will specify the required documentation and records to be submitted in advance or presented on the day of the assessment. The data controller may bring along relevant personnel who can demonstrate compliance, answer questions, and provide clarifications.

Although the assessment occurs at the Authority's premises, the Authority retains the discretion to conduct an on-site evaluation if deemed necessary to validate claims or verify operational practices. Attendance at the Authority's offices for such assessment is mandatory for the data controller upon formal request.

4.3. Virtual Assessment

A virtual assessment is conducted remotely via digital communication tools, including telephone calls, video conferencing platforms (such as Zoom or Microsoft Teams), or email. This method is particularly suitable for preliminary compliance checks, follow-up assessments, or targeted reviews where a physical presence is not immediately required.

Data controllers may be required to submit documentation electronically before the assessment. As with off-site assessments, the Authority reserves the right to conduct a subsequent on-site assessment where additional verification is necessary. Virtual assessments ensure efficiency and accessibility, primarily where geographical or logistical constraints exist.

5. GENERAL ASSESSMENT PROCEDURE

While the specific sequence of activities may vary depending on the type of assessment, the Authority applies a structured and transparent process to ensure fairness and consistency. The general procedure is as follows:

a) Notification (where applicable):

For voluntary and routine planned assessments, the Authority issues formal communication to the data controller confirming or notifying them of the assessment date, time, scope, and the composition of the compliance assessment team. For ad hoc assessments, notification occurs at the point of arrival.

b) Opening Meeting:

The assessment team introduces itself to the accounting officer or the designated contact person of the data controller. The objectives, scope, and methodology of the assessment are outlined, and the data controller is informed of all key requirements, including documentation and personnel expected to participate.

c) Information Gathering:

The assessment team reviews relevant records and documentation, including policies, procedures, contracts, records of processing activities, DPIAs, technical and organisational security measures, and staff training records. This step provides the foundation for assessing compliance with statutory obligations.

d) Interviews:

Discussions are held with key personnel, including the Data Protection Officer (DPO), members of the IT and information security teams, human resources staff, and senior management. These interviews are designed to test understanding, verify implementation of policies, and assess accountability mechanisms.

e) Inspection & Testing:

The team may conduct direct observations, system demonstrations, and technical testing to verify the effectiveness of implemented controls and security safeguards. This includes confirming whether organisational and technical measures are functioning as intended.

f) Closing Meeting:

At the conclusion of the assessment, preliminary findings are shared with the data controller. This provides an opportunity to clarify, correct factual inaccuracies, and, where applicable, discuss initial remedial steps.

g) Reporting:

The Authority shall provide the data controller with a final compliance assessment report within twenty-one (21) days of completing the assessment. The report will set out the key outcomes of the evaluation and serve as a formal record of the data controller's compliance status under the Cyber and Data Protection Act. Each report will include a summary of the overall compliance status, categorised as Compliant, Partially Compliant, or Non-Compliant. It will also present detailed findings and recommendations, identifying specific gaps, suggested remedial actions, responsible persons, and implementation timelines. In addition, the report will include a risk assessment highlighting risks to personal data and prioritising corrective actions based on their potential impact and likelihood of occurrence. Finally, where follow-up assessments are conducted, the Authority will issue a supplementary section or report to confirm whether the identified gaps have been addressed and closed to the Authority's satisfaction.

CONCLUSION

These guidelines provide a clear, transparent framework for conducting compliance assessments under the Cyber and Data Protection Act (CDPA). By outlining the types of assessments, methods, procedures, and reporting requirements, the Authority seeks to ensure consistency, fairness, and accountability in its oversight role. The ultimate objective is not only to enforce compliance but also to support data controllers in building robust governance structures, strengthening organisational practices, and safeguarding the personal information of data subjects.

Through voluntary, routine, and ad hoc assessments, the Authority balances proactive engagement with regulatory vigilance, thereby fostering a culture of continuous improvement in data protection practices across all sectors. The assessment process, combined with transparent reporting and follow-up mechanisms, is intended to promote trust, transparency, and accountability in Zimbabwe's digital ecosystem. In this way, the Authority reaffirms its commitment to protecting the rights and freedoms of individuals while enabling responsible innovation and growth in the digital economy.

For further guidance on licensing requirements and process, contact the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) at regulator@potraz.zw or call +263 242 333032/48 .

Annexure A: Data Protection Compliance Assessment Checklist

Name of Data Controller: _____

Sector: _____

Date of Assessment: _____

Type of Assessment: Voluntary Routine Ad Hoc

Method: Onsite Offsite Virtual

Assessor(s): _____

A. Governance & Accountability

Requirement	Yes/No	Evidence/Remarks
Has the organisation appointed a qualified Data Protection Officer (DPO)?		
Is the organisation registered and licensed by the Authority?		
Are data protection roles and responsibilities clearly defined and documented?		
Is there an approved Data Protection Policy?		
Is there evidence of senior management commitment to the protection compliance?		

Lawful Basis for Processing

Requirement	Yes/No	Evidence/Remarks
Has the organisation identified a lawful basis for each category of processing?		
Is consent obtained where required, and is it specific, informed, and freely given?		
Is there a system to record and manage consents?		

Is data processing limited to the stated purposes?		
Are Data Processing Agreements in place with third parties?		

B. Data Subject Rights

Requirement	Yes/No	Evidence/Remarks
Are there documented procedures for handling data subject rights requests (access, rectification, deletion, objection, etc.)?		
Are requests responded to within 30 Days?		
Is there a record of all rights requests received and actions taken?		

C. Data Security & Breach Management

Requirement	Yes/No	Evidence/Remarks
Are appropriate technical and organisational security measures in place?		
Is there an incident response and breach notification procedure?		
Have staff been trained on breach reporting obligations?		
Are breaches reported to the DPA and affected individuals in line with CDPA requirements?		

D. Cross-Border Data Transfers

Requirement	Yes/No	Evidence/Remarks
Are cross-border transfers conducted only with the prior Authority's authorisation were required?		
Are adequate safeguards (e.g., Standard Contractual Clauses, IDTAs) in place?		
Are data subjects informed of cross-border transfers?		

E. Data Minimisation & Retention

Requirement	Yes/No	Evidence/Remarks
Is only the minimum necessary data collected for each purpose?		
Are retention periods defined and documented?		
Is there a process for the secure disposal of personal data?		

F. Training & Awareness

Requirement	Yes/No	Evidence/Remarks
Have staff received initial and refresher data protection training?		
Is there evidence of training completion records?		
Is data protection awareness included in induction programmes?		

G. Risk Management & DPIAs

Requirement	Yes/No	Evidence/Remarks
Are Data Protection Impact Assessments (DPIAs) conducted for high-risk processing activities?		
Are DPIAs reviewed and updated when necessary?		
Are risks to personal data identified, assessed, and mitigated?		

H. Findings Summary

Compliance Area	Status (Compliant / Partial / Non-Compliant)	Priority (High / Medium / Low)
Governance & Accountability		
Lawful Basis for Processing		
Data Subject Rights		
Data Security & Breach Management		

Cross-Border Data Transfers		
Data Minimisation & Retention		
Training & Awareness		
Risk Management & DPIAs		

Recommendations

(To be completed in a separate Report)

Assessor(s) Name & Signature: _____

Date: _____

Data Protection Compliance Assessment Scoring Checklist

Scoring Method

Yes = 2 points

Partial = 1 point

No = 0 points

Not Applicable (N/A) = Excluded from scoring

Compliance Percentage Formula:

1. Governance & Accountability (Max 10 points)

Requirement	Score (0–2)	Evidence/Remarks
1.1 Appointment of qualified DPO		
1.2 DPO registered with DPA (if applicable)		
1.3 Clear roles & responsibilities documented		
1.4 Approved Data Protection Policy in place		
1.5 Senior management commitment evidenced		

2. Lawful Basis for Processing (Max 10 points)

Requirement	Score (0–2)	Evidence/Remarks
2.1 Lawful basis identified for all processing		
2.2 Consent obtained where required		
2.3 Consent records maintained		
2.4 Processing limited to stated purposes		
2.5 Valid Data Processing Agreements in place		

3. Data Subject Rights (Max 6 points)

Requirement	Score (0–2)	Evidence/Remarks
3.1 Procedures for handling rights requests		
3.2 Requests responded to within timelines		

Requirement	Score (0–2)	Evidence/Remarks
3.3 Record of rights requests maintained		

4. Data Security & Breach Management (Max 10 points)

Requirement	Score (0–2)	Evidence/Remarks
4.1 Adequate technical & organisational measures		
4.2 Incident response & breach procedure		
4.3 Staff trained on breach obligations		
4.4 Breaches reported as required by CDPA		

5. Cross-Border Data Transfers (Max 10 points)

Requirement	Score (0–2)	Evidence/Remarks
5.1 DPA authorisation obtained where required		
5.2 Adequate safeguards in place		
5.3 Data subjects informed of transfers		

6. Data Minimisation & Rétention (Max 10 points)

Requirement	Score (0–2)	Evidence/Remarks
6.1 Only minimum data collected		
6.2 Retention periods defined		
6.3 Secure disposal process in place		

7. Training & Awareness (Max 10 points)

Requirement	Score (0–2)	Evidence/Remarks
7.1 Staff receive training		
7.2 Training records maintained		
7.3 Induction includes data protection		

8. Risk Management & DPIAs (Max 10 points)

Requirement	Score (0–2)	Evidence/Remarks
8.1 DPIAs conducted for high-risk processing		
8.2 DPIAs reviewed/updated when necessary		
8.3 Risks identified and mitigated		

SUMMARY SCORING TABLE

Section	Max Points	Points Scored	Compliance % per Section
Governance & Accountability	10		
Lawful Basis for Processing	10		
Data Subject Rights	10		
Data Security & Breach Management	10		
Cross-Border Data Transfers	10		
Data Minimisation & Retention	10		

Section	Max Points	Points Scored	Compliance % per Section
Training & Awareness	10		
Risk Management & DPIAs	10		

Overall Compliance %: _____

Compliance Status Legend

90–100% = Fully Compliant

70–89% = Substantially Compliant (Minor Improvements Needed)

50–69% = Partially Compliant (Significant Improvements Needed)

Below 50% = Non-Compliant (Urgent Action Required)

Implementation Guidelines on Continuous Professional Development Assessment for Certified Data Protection Officers

CDPG 2 of 2025



Implementation Guidelines on Continuous Professional Development Assessment for Certified Data Protection Officers

1. Purpose

These guidelines are in terms of section 20(5) of the Cyber and Data Protection Act, which empowers the Authority to make guidelines for the qualifications of the DPO. Data Protection Officers (DPOs) who are certified in terms of Section 13(2) of S.I. 155 of 2024. It ensures DPOs maintain up-to-date knowledge and practical skills in data protection and other related matters.

2. Scope

These guidelines apply to all individuals who hold the Data Protection Certification and who intend to maintain authorisation to practice as a DPO in Zimbabwe.

3. Key Principles

a) Certified DPO must undertake continuous learning and development to continue practising as such.
b) DPOs must earn 12 CPD points each calendar year to maintain their certification in good standing.
c) To guarantee quality and consistency, CPD activities are primarily drawn from Authority-organised events, while external events only qualify if they have been formally accredited by the Authority. This approach ensures regulator-led quality assurance and protects the integrity of the programme.
d) The CPD framework is also competency-focused, designed, with particular emphasis on artificial intelligence governance and cybersecurity/breach response.

3. Definitions:

a) CPD point (also “CPE point”): A unit of professional learning earned through qualifying activities. Four (4) contact hours = 1 CPD point. Points may be recorded in quarter-point increments (e.g., 1 hour = 0.25 point).

b) Calendar year: 1 January – 31 December.

c) Accredited provider: An organisation whose event has been approved by POTRAZ for CPD credit.

d) AI governance: Policies, processes, and controls for the safe, lawful, and ethical design, deployment, and oversight of AI systems.

e) Cybersecurity & breach management: Risk management, incident response, forensics, reporting/ notification, and lessons learned.

4. Annual CPD Requirement

Each certified DPO is required to earn 12 CPD points per calendar year, with a structured allocation to ensure balanced professional development. At least 4 points must be in the privacy framework, and another 4 points in Breach Management. In comparison, the remaining 4 points may be obtained from any other approved

data-protection-related topics, such as privacy law updates, Data Protection Impact Assessments (DPIAs), children's data, cross-border data transfers, ethics, or records management. For certifications granted mid-year, the CPD requirement is pro-rated at 1 point per full calendar month of certification remaining in that year, with proportional expectations for privacy framework and breach management content, rounded to the nearest 0.25 point to ensure fairness and consistency. A DPO is not required to earn the CPD points in the year that they obtain their certification. You are also required to attend at least one major Authority event such as the annual symposium.

5. Qualifying Activities & Points

1.1 CPD points may be earned through three main categories of activities. First, participation in Authority's events, such as conferences, workshops, symposiums, and webinars, is automatically eligible, with credit awarded at the rate of 1 point per 4 contact hours (0.25 per hour).

1.2 Events organised by other institutions—whether local, regional, or international—are also eligible for credit, provided they are formally accredited by the Authority in accordance with Section 7, and they follow the same points allocation system of 1 point per 4 contact hours.

1.3 To encourage diverse forms of professional growth, certain additional contributory activities may also count towards CPD, though these are capped at a total of 4 points per year within the 12-point requirement. These include :

1.3.1 speaking or delivering training, credited at 0.75 points per hour with a maximum of 3 points annually;

1.3.2 scholarly or professional writing, where peer-reviewed journal articles or book chapters earn 2 points each (maximum 2 points per year), and practice articles, guidance notes, or equivalent works of at least 1,200 words earn 1 point each (maximum 2 points per year); and

1.3.3 structured self-study, such as reading major standards or official guidance of 10,000 words or more, or completing a graded e-module/assessment, credited at 0.5 point each (maximum 2 points annually).

1.4 To preserve rigour and consistency, at least 8 of the 12 required points must come from live or structured events (POTRAZ or POTRAZ-accredited), while the remaining up to 4 points may be earned through the contributory activities outlined above.

6. Accreditation of Non-POTRAZ Events.

a) Organisers seeking CPD accreditation must submit their request to the Authority (or via the CPD portal once operational) no later than 21 calendar days before the event.

b) The submission must include a concept note outlining the learning objectives, target audience, agenda with time allocations, delivery method, and any assessments to be used.

c) It should also contain detailed speaker profiles or CVs highlighting qualifications, experience, affiliations, potential conflicts of interest, and prior speaking engagements.

d) In addition, organisers must provide draft materials or a reading list, an evaluation form, and a clear attendance verification plan (e.g., sign-in sheets, platform logs, or proctoring measures).

e) Accreditation decisions will be based on several factors, including the relevance of the content to Zimbabwe's Cyber and Data Protection Act and its associated regulations or guidelines.

f) Consideration will also be given to academic and professional rigour, including the clarity of learning outcomes, qualifications of speakers, and reliability of sources.

g) Other evaluation factors include the duration, interactivity, and assessment methods of the

programme, as well as the integrity of the provider, ensuring impartiality of content and full disclosure of sponsorships or conflicts of interest.

h) If the event meets the required standards, POTRAZ will issue an Accreditation Letter together with a unique Event CPD Code. This code will specify the number of approved hours, the topic classification and the equivalent CPD points.

i) Within 10 working days after the event, organisers are required to submit a package of post-event materials, including a signed attendance register or platform participation logs, the final programme and slides, a summary of participant feedback, and copies of certificates of attendance issued to delegates, each of which must display the Authority's Event CPD Code.

7. Evidence & Submission by DPOs

DPOs are required to submit their CPD evidence to the Authority by 31 December following the end of each CPD year, which runs from 1 January to 31 December. The submission pack may be uploaded via the CPD portal or sent by email and must include a completed CPD Summary Log (using the official Authority's template), certificates of attendance or transcripts, accreditation references (Authority's Event CPD Code or Accreditation Letter), and, where contributory activities are claimed, supporting documentation such as a copy of the publication (or DOI/URL), a conference agenda showing the DPO as a listed speaker, or completion/assessment records. All DPOs are required to retain their underlying evidence for at least 24 months, as it may be requested during an audit.

8. Point Calculation Rules

For CPD allocation, 60 minutes of learning equals one contact hour, excluding breaks longer than 10 minutes. CPD points may be rounded to the nearest 0.25 point. Attendance at identical or substantively similar content more than once in the same year will not be credited, as duplicative learning does not count towards annual requirements. Additionally, up to three CPD points earned between October and December may be carried over into the next CPD year.

9. Quality Assurance, Audit & Misrepresentation

The Authority reserves the right to conduct random or risk-based audits of CPD submissions at any time, requesting corroborating evidence to verify compliance. Outcomes of these audits may include acceptance of the submission, a request for further documentation to be provided within 30 days, or denial of credits where insufficient proof exists. Any false claims or forged evidence will result in immediate sanction under this guideline (see Section 12 of these guidelines) and may also be referred for enforcement under applicable law or professional codes.

10. Roles & Responsibilities

DPOs are responsible for planning their annual learning, identifying and addressing competency gaps, earning the required points, maintaining accurate records, submitting evidence on time, and upholding professional ethics. POTRAZ, as the regulatory authority, will publish annual CPD priority themes, accredit non-POTRAZ events, maintain the CPD portal and related processes, audit submissions, and issue or

withdraw good-standing status as necessary. Event organisers and providers are responsible for ensuring their programmes meet required standards of quality, that qualified speakers are engaged, that accurate attendance records are kept, and that all post-event reporting obligations are fulfilled.

11. Non-Compliance & Sanctions

1.1 If a DPO fails to meet the 12-point annual requirement by 31 January, their certification status will automatically be changed to Suspended, meaning they are no longer authorised to practice until compliance is achieved.

1.2 Continued non-compliance beyond 31 March will result in the cancellation of certification, and the individual will no longer be authorised to act as a DPO in Zimbabwe.

1.3 Reinstatement after cancellation will require full re-certification, which includes meeting the current entry requirements and may also involve the payment of an administrative fee.

12. Waivers, Deferrals & Special Circumstances

In exceptional cases such as serious illness, bereavement, parental leave, or other extraordinary circumstances, DPOs may apply for a waiver or deferral. Requests must be submitted to the Authority in writing, supported by appropriate documentation, by 31 January. Where granted, Authority may either defer the submission deadline or pro-rate the CPD requirement for that year. Generally, the maximum allowable deferral is 12 months.

13. Ethics, Conflicts of Interest & Independence

DPOs must conduct themselves with integrity, avoiding any conflicts of interest that could compromise their independence or breach confidentiality. Event sponsors must always be disclosed, and purely marketing-oriented content will not qualify for CPD credit unless it is clearly educational in nature and independently curated.

14. Communication of Status

To promote transparency and accountability, the Authority will maintain a register of certified DPOs in good standing. Employers, organisations, and data controllers may verify the status of a DPO through this register or by requesting written confirmation directly from the Authority.

15. Data Protection & Records

All CPD submissions will be processed by the Authority in line with applicable data protection laws. Records will be retained only for as long as necessary to fulfil regulatory purposes, including audits, dispute resolution, or enforcement actions.

16. Disputes & Appeals

DPOs who disagree with a CPD-related decision may first seek informal resolution by contacting the Authority's CPD administration within 30 days of the decision. If the matter remains unresolved, a formal appeal may be lodged with the Authority's Certification Committee within 30 days of the informal outcome,

supported by objective evidence. Appeals will be reviewed by an independent panel, and the decision of that panel will be final.

17. Guidelines Review

These guidelines are subject to annual review to ensure they remain aligned with legislative developments, technological advancements, and professional best practices. The Authority will notify all certified DPOs of any material amendments and their effective dates.

For further guidance on licensing requirements and process, contact the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) at regulator@potraz.zw or call +263 242 333032/48 .

Implementation Guidelines on how to conduct a Data Protection Impact Assesment (DPIA)

CDPG 3 of 2025



Implementation Guidelines on How to Conduct a Data Protection Impact Assessment (DPIA)

1. Purpose And Effective Date

These guidelines are issued in accordance with section 18 of the Cyber and Data Protection Act [Chapter 12:07] (hereinafter referred to as "the CDPA"). The CDPA mandates the Authority to produce guidelines to facilitate and promote the fair processing of personal data in Zimbabwe. These guidelines seek to assist data controllers in conducting Data Protection Impact Assessments (DPIAs to promote compliance with the law and to promote responsible data governance. The Guidelines shall take effect on the date of publication.

2. INTERPRETATION

In these Guidelines, the following shall mean:

"CDPA" refers to the Cyber and Data Protection Act [Chapter 12:07]

"Data Protection Authority (DPA) or "the Authority" refers to the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), designated as such in terms of section 5 of the Cyber and Data Protection Act.

"DPIA" refers to a Data Protection Impact Assessment

"Data Controller" refers to any natural person or legal person who is licensable by the Authority, including public bodies and any other person who determines the purpose and means of processing personal data.

"Data protection officer" or "DPO" refers to any individual appointed by the data

controller and who is charged with ensuring, in an independent manner, compliance with the obligations provided for in the CDPA.

"Personal information" means information relating to a data subject which can be used to identify an individual.

"Processing" refers to any operation or set of operations which are performed upon data, whether or not by automatic means, such as obtaining, recording or holding the data or carrying out any operation or set of operations on data.

"Data Subject" means an identified or identifiable natural person who is the subject of data.

"Sensitive data" refers to information or any opinion about an individual which reveals or contains, racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sex life; criminal, educational, financial or employment history; gender, age, marital status or family status.

"Transborder flow" refers to international flows of data by means of transmission, including data transmission electronically or by satellite.

"Risk" refers to the likelihood and impact of harm that may result from the processing of personal data.

"Risk assessment" refers to identifying, assessing, and mitigating potential risks associated with certain processing activities.

3. LEGAL FRAMEWORK

These guidelines are grounded in:

1. Section 18 (2) of the Cyber and Data Protection Act [Chapter 12:07] (CDPA) which requires data controller to into account measures that balance the need for processing data and the need to mitigate the risks to the rights of the data subjects.
2. Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations, 2024

They can be read with the following:

3. Implementation Guidelines Implementation Guideline on Cross-Border Transfer of Personal Information (CDPG 5 of 2024)
4. Implementation guideline Implementation Guideline on the Right to Consent (CDPG 4 of 2024)
5. Cyber and Data Protection Implementations Guidelines on Appointment, Roles, Responsibilities, Training and Certification of Data Protection Officers (CDPG1 of 2024).
6. Cyber and Data Protection Implementations Guidelines on Processing of Children's Personal Information (CDPG 2 of 2024).

4. INTRODUCTION

A DPIA is a systematic process employed to identify, assess and mitigate the privacy risks associated with a specific data processing activity. It serves as a significant tool in demonstrating compliance with the CDPA, and it promotes the safeguarding of data subjects' privacy rights and freedoms outlined in terms of sections 14,11, and 25 of the CDPA.

5. IMPORTANCE OF CONDUCTING A DPIA

5.1. DPIAs are an essential part of a data controller's accountability obligations.

5.2. Conducting a DPIA is a legal requirement in terms of section 18 of the CDPA; as a DPIA is a form of organisational measure that seeks to identify risks for specified types of processing that are likely to adversely impact the rights and freedoms of individuals.

5.3. DPIAs play a key role in raising awareness about privacy and data protection within an organisation.

5.4. Beyond meeting legal requirements in terms of the Act, DPIAs offer broader compliance advantages by helping data controllers to evaluate and demonstrate adherence to data protection principles and responsibilities.

5.5. DPIAs are more than just a regulatory formality because when done effectively, they help identify and resolve potential risks to data privacy early, benefiting both individuals and the

organisations.

5.6. Conducting a DPIA can also reassure data subjects that their data is being handled responsibly and that any risks to them have been minimised.

5.7. Conducting DPIAs can help a data controller to embed privacy by design and default at the beginning of high-risk processing activities.

6. PURPOSE OF A DPIA

6.1. As emphasised above, DPIA is an important tool to demonstrate compliance with the law in line with the principle of accountability enshrined in section 24 of the CDPA; however, it should not be viewed as a one-time exercise.

6.2. It should be a 'living' document that helps a data controller to manage and review the risks of a processing activity, and the effectiveness of measures put in place to mitigate the identified risks on an ongoing basis throughout the lifecycle of the processing activity.

7. INSTANCES WHEN A DPIA SHOULD BE CONDUCTED

7.1. A DPIA is a mandatory requirement where a type of processing activity is, after taking into account the nature, scope, context and purposes of the processing, likely to result in a high risk to the rights and freedoms of data subjects.

7.2. It is part of the mandatory requirement in terms of section 18 of the CDPA.

7.3. A DPIA is mandatory when:

- Processing involves sensitive personal data as defined in sections 11 and 12 of the Act
- Processing involves cross-border transfer of personal data in terms of sections 28 and 29 of the CDPA.
- The transborder notification of processing of data to the Authority must be accompanied by a DPIA.
- There is large-scale profiling or automated decision-making
- Surveillance or monitoring of public spaces occurs
- Data subjects include vulnerable groups (e.g., children, the elderly)
- New technologies are deployed in a business (e.g., Biometrics, AI, IoT)
- When the Authority calls upon a data controller to conduct a DPIA

8. PRACTICAL STEPS TO FOLLOW WHEN CONDUCTING A DPIA

Step 1: Identify the need for a DPIA

The first step is to determine if a DPIA is necessary.
Use a screening checklist as provided in section 7 of these Guidelines.

Step 2: Describe the processing

Provide a clear description of the data processing activities, including but not limited to;

- Types of personal data being processed,
- Lawful basis for processing
- Purpose of processing
- Data sources and data recipients,

- Data Sharing protocols and involvement of third parties
- Data retention and deletion schedules specify how long the data will be kept and when it will be deleted.

Step 3: Consultation

Consult internal and external stakeholders, ie DPO, project owners, managers, industry experts, IT professionals, legal advisors, user departments, data processors, and data subjects.
Consult and seek expert guidance from the DPA where necessary.
Define roles and responsibilities.

Step 4: Assess necessity and proportionality

Evaluate whether there are other alternative ways to achieve the same goal with less data or lower risks.
Assess compliance with data protection principles as enshrined in the CDPA.

Step 5: identify and assess risks

Identify risks, risk level vis-à-vis a vee nature of processing and the level of sensitivity of the data as provided herein in section 9.
The use of risk assessment tools such as specialised software to generate standardised reports is encouraged.

Step 6: Identify measures to mitigate risks

After identifying risks, set up measures to mitigate them.

Implement technical and organisational measures to secure the security

and confidentiality of data.

Step 7: Sign off and record outcomes

Maintain all documentation

Submit the DPIA to the Authority if it's necessary in terms of the law

Map a strategy for the implementation of identified outcomes

9. WAYS OF ASSESSING RISKS IN DATA PROCESSING ACTIVITIES WHEN CONDUCTING A DPIA

9.1. Mapping of the Data Flow

9.1.1. The data controller can assess risks in processing activities by doing a data inventory focusing primarily on;

- Type of personal data involved
- Amount and range of data handled
- Level of sensitivity
- the extent and frequency of processing
- the duration of processing
- the geographical area covered

9.1.2. Risks can be classified into three categories, ie, Low, medium and high and risk

classification is important as it guides the data controller on the implementation of appropriate organisational and technical measures to employ on different sets of processing activities.

9.1.3. It is important to map out the data accurately, setting out data collection, processing, and storage to reveal any weak points or vulnerabilities.

9.2. Scope of impact

9.2.1. The Data controller should ensure that a comprehensive assessment of the potential impact on the rights and freedoms of individuals is conducted.

9.2.2. This assessment must be in light of the harm or damage a certain processing activity may cause, whether physical, emotional or material. In particular, the assessment can primarily focus on whether the processing could contribute to;

- inability of data subjects to exercise their rights
- inability of individuals to access services or opportunities;
- loss of control or autonomy by data subjects over the use of their personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage.

9.3. Data controllers can also assess risks considering their standing in society as a corporate institution, for example, the impact of regulatory action by the DPA on their operations, reputation, and public trust.

10. EXAMPLES OF HIGH-RISK PROCESSING ACTIVITIES

High-risk processing activities include the following:

10.1. When processing involves the use of automated systems, innovative technologies, or the novel application of existing technologies (including AI).

10.2. When decisions about an individual's access to a product, service, opportunity or benefit are based on automated decision-making.

10.3. When processing involves any profiling of individuals on a large scale.

10.4. When processing involves health, biometric and genetic data or any of the sensitive data in terms of section 3 of the CDPA.

10.5. When personal data, obtained from multiple sources, is combined, compared or matched in one processing activity.

10.6. When processing of personal data has not been obtained directly from the data subject in circumstances in terms of section 16 of the CDPA.

10.7. When processing involves tracking an individual's geolocation or behaviour.

10.8. When processing involves children's information or any other vulnerable data subjects.

10.9. Where the processing is of such a nature that a personal data breach could jeopardise the

health or safety of individuals.

11. ROLE OF A DATA PROTECTION OFFICER (DPOs) IN CONDUCTING A DPIA

11.1. The DPO plays a pivotal role in assisting the Data Controller in conducting a DPIA

11.2. The DPO **does not** conduct the DPIA. The Data Controller must conduct the DPIA.

11.3. In conducting a DPIA, the DPO's role is advisory and they

a. Guide the process by identifying the need for a DPIA.
b. Assisting in the documentation of the DPIA process.
c. Assisting in risk assessment to identify the risks inherent in data processing
d. Advising on risk mitigation measures
e. Monitor the adherence and compliance to the outcomes, findings and the DPIA to ensure that there is implementation of all technical and organisational measures as rolled out or planned.

12. DPIA CHECKLIST/CONTENT REQUIREMENTS

A comprehensive DPIA is expected to provide adequate information on the following:

- Overview: Title and description of the processing activity, objectives and expected outcomes.
- Data Inventory: Categories of data collected and data flow diagram (collection, storage, sharing, disposal).
- Data Subjects: a list and category of data subjects whose personal information will be processed.
- Establishment of a legal basis: Consent, contractual obligation, legal obligation, public interest, vital interest of data subject, legitimate interest.
- Evidence and results of consultation: Engagement with internal and external stakeholders, data subjects, designation of roles and responsibilities/ ownership of processing activity.
- Adequacy assessment: in terms of section 28 of the Act, in cases of cross-border transfer of data
- Risk Assessment: Identification of risks and their likelihood to adversely affect data subjects, classification of identified risks, for example, (high/medium and low), and likelihood and severity of harm.
- Mitigation Measures: Technical and organisational safeguards implemented,
- Necessary Approvals: Sign-off by Data Protection Officer (DPO), Authorised representatives of the Controller, date and version control and submission to the DPA for assessment/ approval if the DPIA is an annexure to a notification required in terms of section 20 of the Act.

12.1. A DPIA submitted to the Authority, accompanying a specific notification arising from an obligation in terms of the Act, should be accompanied by an annexure of source documents which serve as a demonstration of proof and the accuracy of the DPIA.

12.2. Examples of these documents may include:

- Adequacy assessment demonstrating data residency in cross-border processing of data
- Data processing/ sharing agreements with data processors
- Consent forms when processing sensitive data.

12.3. Before submission of a DPIA to the Authority, the data controller must ensure that it encompasses all the information provided above.

13. RECOMMENDED BEST PRACTICES IN CONDUCTING A DPIA

13.1. Stakeholder Engagement

- When conducting a DPIA, it is important to use accurate and timely information from all relevant stakeholders; therefore, all relevant stakeholders in an organisation should be involved.
- As emphasised, the DPO's advice is very crucial in determining whether a certain processing activity needs a prior conducting of a DPIA, and how to conduct the same.
- Relevant project team and relevant departments should work in consultation with the DPO.
- A wide internal consultation can uncover data protection risks that might only be apparent to individuals working on specific aspects of the project.
- It is also important to consult the DPA, if necessary, to seek additional expert advice and guidance.
- This might include bringing in external specialists if our organisation lacks sufficient expertise or if a project holds a very high level of risk. We should also think about how to consult individuals or their representatives, perhaps through focus groups or surveys.

13.2. Documentation and Record Keeping

- Record keeping is essential for demonstrating compliance with the DPA; therefore, data controllers are encouraged to keep detailed and updated records of the DPIA process.
- The exercise can also be a key identifier of gaps which can be used to monitor the level of compliance for an organisation, in the same vein, fostering review and improvements.

13.3. Continuous Review

- A DPIA is not a one-time exercise; it is an ongoing process that needs to be integrated into the data controller's organisational processes.
- The tool assists controllers in staying on top of changing risks and ensuring that data protection measures remain effective.
- A strategic review of the DPIA in a processing activity enables effective monitoring of the
- Data controllers are encouraged to set review schedules to keep track of any actions that result from the same.
- A DPIA should be conducted when there is a modification to the processing of personal data. The modification should be notified to the Authority, outlining the nature, scope, context, or purposes of processing/ modification.

14. PENALTIES AND FINES FOR NON-COMPLIANCE

Failure to conduct a DPIA when required may result in;

a) Fines up to level 11,

b) Imprisonment up to 7 years

c) An order to stop the processing of personal data- (Cancellation of Data Protection License.)

For compliance and further guidance, contact the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) on regulator@potraz.zw or call +263 242 333032/48

Implementation Guidelines on Adequate Level Of Protection Under Cross-Border Data Transfers

CDPG 4 of 2025



Implementation Guidelines on Adequate Level of Protection Under Cross-Border Data Transfers

1. PURPOSE

These guidelines are issued in terms of Section 6(1) (a) as read with 28 (2) of the Cyber and Data Protection Act [Chapter 12:07] (hereinafter referred to as "the CDPA"), which provides that the Authority shall lay down the conditions and circumstances for cross-border transfer of personal information. They are designed to ensure that cross-border transfers of personal data from Zimbabwe are conducted in a manner that guarantees an adequate protection level to data subjects' personal data, in line with the Cyber and Data Protection Act,, its Regulations, as well as international best practices.

2. INTRODUCTION

The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) is the designated Data Protection Authority. According to Section 28, POTRAZ is responsible for specifying the categories of data that can be transferred outside Zimbabwe and the conditions under which they can be transferred. The reason for restrictions under cross-border transfer provisions in sections 28 and 29 is to guarantee that the personal data being transferred will receive a level of protection comparable to that afforded in Zimbabwe under the CDPA. These guidelines can be read with the Implementation Guidelines on Cross-Border Transfer of Personal Information (CDPG 5 of 2024) It is highly recommended that data controllers adopt the practices outlined in these guidelines as a crucial aspect of their statutory responsibility to safeguard personal data.

3. DEFINITION OF TERMS

a. Act: Refers to the Cyber and Data Protection Act [Chapter 12:07] (CDPA) of Zimbabwe or any relevant legislation governing data protection.
b. Data Controller: A person or entity that determines the purpose and means of processing personal data.
c. Data Processor: A person or entity that processes personal data on behalf of the data controller.
d. Personal Data: Any information relating to an identified or identifiable individual
e. Processing: Any operation performed on personal data, such as collection, storage, use, deletion, and transfer.
f. Sensitive Personal Data: Sensitive Information: refers to personal data that includes biometric data, racial or ethnic origin, political opinions, membership of a political association, and any information that may be considered to present a major risk to the rights of the data subject.
g. Cross-border transfer: refers to the movement of personal data from Zimbabwe to another country's geographical, technological, and legal borders

4. REQUIREMENTS FOR TRANSFER

Data controllers are prohibited from transferring the personal information of data subjects to a third party outside Zimbabwe to a country that does not ensure an adequate level of protection. The data controller must first notify the Authority of their intention to transfer data and must then meet the following conditions before they receive the authorisation to transfer data from Zimbabwe:

4.1 General Principle

No personal data shall be transferred outside Zimbabwe unless the destination country ensures an adequate level of protection for the data subject's rights and freedoms.

4.2 Assessment of Adequacy

Data controllers must assess the adequacy of protection in the destination country based on:

a. Legal Framework: Existence of data protection laws, independent supervisory authority, and enforcement mechanisms
b. Data Subject Rights: Right to access, rectify, erase, and object; remedies for violations
c. Security Measures: Technical and organisational safeguards; breach notification protocols
d. International Commitments: Participation in international data protection agreements (e.g., Malabo Convention on Cyber and Data Protection)

4.3 Transfer Mechanisms

If adequacy is not established, data controllers must use alternative safeguards, such as:

a. Standard Contractual Clauses (SCCs)
b. Binding Corporate Rules (BCRs)
c. Explicit Consent from the data subject
d. Approved Codes of Conduct or Certification Mechanisms

4.4 Documentation & Notification

Data controllers must:

a. Maintain records of cross-border transfers
b. Notify the Data Protection Authority (DPA) before initiating transfers
c. Submit Data Transfer Impact Assessments (DTIA)

4.5 Compliance Assessment

As per SI 155 of 2024 and the Act, Data Controllers must:

a. Be licensed by the Authority.
b. Appoint a Data Protection Officer (DPO) and notify the Authority.
c. Report data breaches within 24 hours.
d. Notify the Authority of the intention to transfer personal data outside of Zimbabwe.
e. Maintain a record of processing activities (ROPA).

4.6 Technical and Organisational Safeguards

To ensure an adequate level of protection during cross-border data transfers, organisations must implement robust technical and organisational measures designed to safeguard personal data against unauthorised access, loss, or misuse. These measures should include, but are not limited to, the following:

a. Encryption

Implement robust end-to-end encryption to protect personal data both during transmission and while at rest. This ensures that data remains confidential and secure, even if intercepted or accessed without authorisation.

b. Data Minimisation

Limit the collection and transfer of personal data to only what is strictly necessary for the intended purpose (data minimisation). Apply pseudonymisation to reduce the risk of re-identification, especially when transmitting sensitive or high-risk data across borders.

c. Access Control Mechanisms

Enforce strict access control mechanisms, including role-based access and multi-factor authentication (MFA), to ensure that only authorised personnel can access or process personal data. Access rights should be regularly reviewed and updated.

d. Monitoring logs

Maintain comprehensive monitoring systems and audit logs for all cross-border data transfers. Logs should capture when, where, and how personal data is transferred, along with details of the data recipient. This supports accountability, traceability, and incident investigation.

e. Incident response plan

Establish and maintain a security incident response plan that includes timely detection, reporting, containment, and remediation of data breaches. In the event of a breach involving cross-border data, notify the appropriate supervisory authority and affected data subjects in accordance with applicable legal and regulatory requirements.

f. Sensitive Information

The Authority will not permit the migration or hosting of highly sensitive information, such as core banking platforms and critical financial systems, outside the borders of Zimbabwe. All such systems must be hosted locally, and any exceptions will require prior written approval from the Authority, supported by a detailed risk assessment and justification.

g. Security Audits

Regular audits and penetration testing are essential components of a robust data protection framework, particularly where cross-border data transfers are involved. Audits help assess compliance with legal, regulatory, and contractual obligations, ensuring that data protection controls such as encryption, access management, and third-party agreements are effectively implemented and maintained.

h. For cross-border data transfers, penetration testing conducted periodically will enhance the organisation's capability to identify and mitigate security vulnerabilities, thereby preventing potential breaches. This proactive approach not only demonstrates accountability but also helps ensure the ongoing integrity and confidentiality of personal data as it moves across international boundaries.

4.7 Security Standards

In addition, the data controller should ensure that third-party recipients adopt the following standards:

a. ISO/IEC 27001 for information security

b. NIST SP 800-61 – Computer Security Incident Handling Guide
c. ISO/IEC 27036 – Information Security for Supplier Relationships

4.8 Penalties or Fines for Non-Compliance

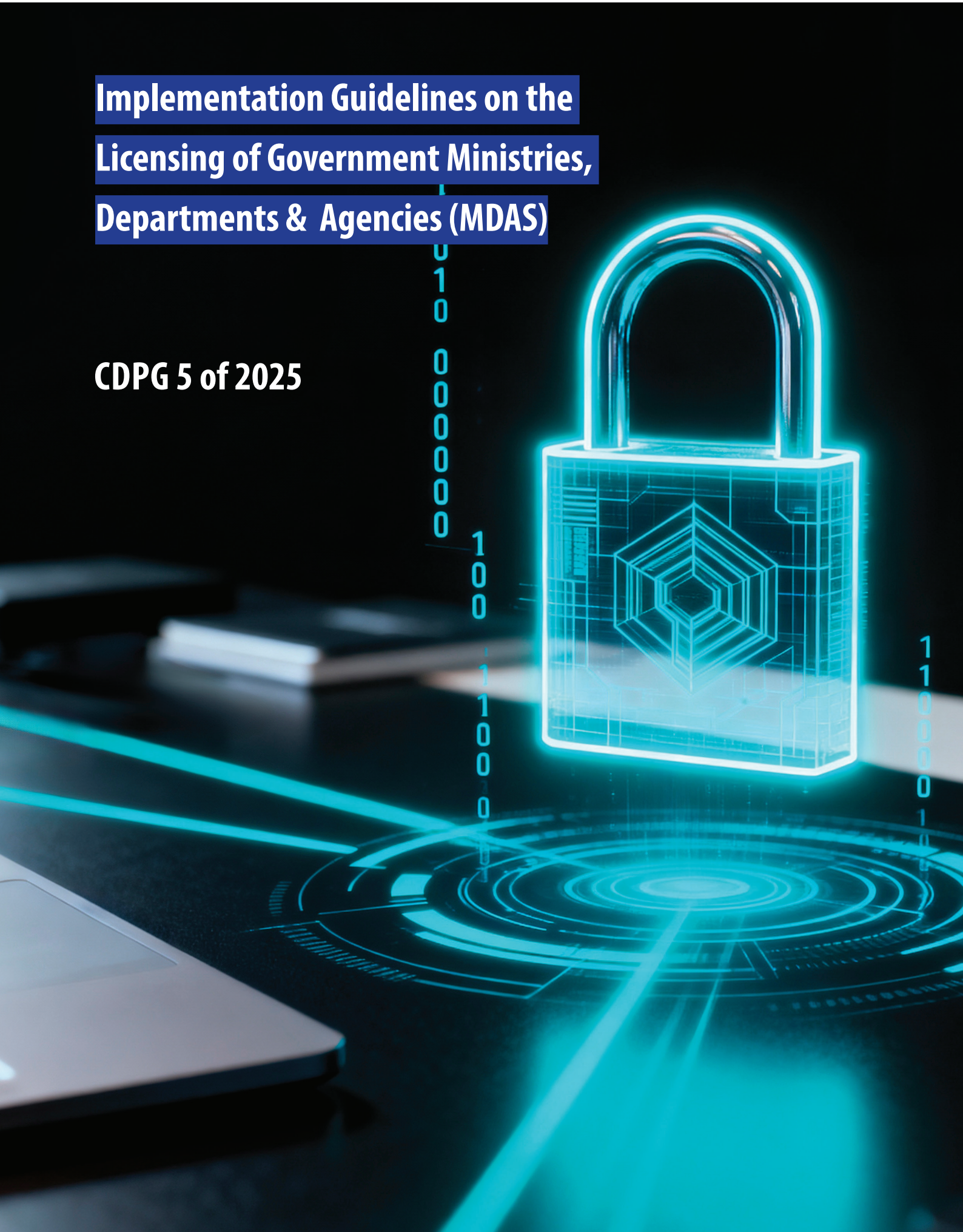
A data controller who shall not guarantee the above required minimum adequate level of protection shall attract the following fines or penalties:

a. Fines up to level 11
b. Imprisonment up to 7 years
c. Revocation of data controller license

For complaints and further guidance, contact the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) at regulator@potraz.zw or call +263 242 333032/46/48.

Implementation Guidelines on the Licensing of Government Ministries, Departments & Agencies (MDAS)

CDPG 5 of 2025



Implementation Guidelines on the Licensing of Government Ministries, Departments & Agencies (MDAS)

Issued in terms of the Cyber and Data Protection Act [Chapter 12:07] (CDPA) as read together with Statutory Instrument 155 of 2024 – Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations, 2024

1. INTRODUCTION

These guidelines outline the procedure and requirements for the licensing of Government Ministries, Departments & Agencies (MDAs) as data controllers under Zimbabwe's data protection legal framework. It is aimed at facilitating compliance with the Cyber and Data Protection Act and ensuring that MDAs operate within the bounds of lawful data processing.

These guidelines serve to clarify how MDAs should apply for data controller licenses and the conditions under which Data Protection Officers (DPOs) should be appointed.

2. DEFINITIONS

For these guidelines, the following definitions shall apply:

- Agency: Refers to any organisation or body that is established or functions as part of the government or public sector and is responsible for administering or providing services in the public interest. An Act of Parliament must establish an agency. Agencies include Independent Commissions, Boards and Authorities.
- Government Department: A functional branch or administrative unit within a government ministry that carries out specified duties or responsibilities in line with the ministry's broader mandate.
- Ministry: a specialised government unit which is responsible for a broad administrative function within the Executive arm of government, which a line minister heads.
- Public Authority: Refers to any organisation or body that is established by an Act of Parliament, which functions as part of the government or public sector and is responsible for administering or providing services in the public interest.
- State-Owned Enterprise (SOE) means a legal entity in which the State holds a majority ownership interest, whether directly or indirectly, and which engages in commercial or public service activities on behalf of the Government of Zimbabwe.
- Parastatal means a statutory body or corporation established by an Act of Parliament to perform specific governmental or public interest functions under ministerial supervision, and which operates with partial or complete financial support from the State.
- Polytechnic means a tertiary education institution that provides applied science, engineering, or technological education and training, usually offering diploma and degree-level programmes in technical and vocational disciplines.

3. ARE MDAs REQUIRED TO OBTAIN DATA CONTROLLING LICENSES?

3.1 In terms of Section 3 of the CDPA, public authorities who control the means of processing data are licensable by the Authority. MDAs are public authorities and must obtain a data control license under Section 4 of the Regulations.

3.2 There is no exemption on the licensing of MDAs in terms of Section 8 (1) of the Regulations. The exemption is only for personal, family, or household use, law enforcement, and journalistic or archival purposes.

3.3 MDAs are therefore required to obtain a data controlling license.

4. HOW CAN MDAs OBTAIN DATA CONTROLLING LICENSES

4.1 Every line ministry shall apply for a data processing license.

4.2 Government Departments are administrative units of Ministries, but do not have a separate legal persona; therefore, they are licensable by the Authority.

4.3 Agencies are separate legal entities and, as such, are licensable by the Authority.

4.4 When a Ministry applies for a data controller license, the license shall cover the Ministry and all its Departments.

4.5 The application shall be on a special form DP1 A.

4.6 A license will be issued in the name of the Ministry and shall be deemed to include all the Departments under the Ministry.

5. APPOINTMENT OF DATA PROTECTION OFFICERS (DPOS) IN MINISTRIES

5.1 Every Ministry is required to appoint a Data Protection Officer (DPO).

5.2 The DPO must be trained and licensed by the Authority in terms of Section 13 (2) of the Regulations.

6. LICENSING OF AGENCIES AND PUBLIC AUTHORITIES

6.1 All Agencies and Public Authorities that are separately incorporated or registered under any law of Zimbabwe shall be treated as independent data controllers.

6.2 These entities must apply for licenses in their own capacity, even if they fall under the general oversight of a parent ministry.

6.3 This distinction is made because they possess separate legal personality and manage their own data independently.

7. GENERAL REQUIREMENTS FOR ALL MDAs

According to Section 5 of the Regulations:

7.1 All MDAs must renew their data controlling licenses annually.

7.2 All data controlling licenses must be renewed at least 3 months before the expiry of the data controlling license.

POTRAZ shall be responsible for monitoring compliance with the licensing requirements under this guideline. Monitoring shall include periodic inspections, submission of compliance reports, and targeted reviews to ensure that all licensed institutions maintain appropriate technical and

organisational measures for data protection. The regulator shall also provide compliance feedback and capacity-building support where necessary.

8. AUDITS AND ASSESSMENTS

Licensed MDAs shall be subject to technical audits and compliance assessments to evaluate the adequacy of their data protection and information security controls. Such audits may include vulnerability testing, system reviews, and data handling evaluations conducted by POTRAZ or its appointed auditors. The outcome of each assessment shall form part of the institution's compliance record and may influence renewal or suspension decisions.

9. OFFENCES

9.1 Any MDAs that fail to obtain a data controlling license within the stipulated timeframes 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.

9.2 Any MDAs that fail to renew their data controlling license without just cause 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.

9.3 Any MDAs that fail to appoint a DPO within the stipulated period shall be guilty of an offence and liable to a fine not exceeding level 7 or to imprisonment not exceeding two years or to both such fine and such imprisonment.

10. INSTITUTIONAL EFFICIENCY

Institutions that are not separate legal entities shall operate under the license of their parent institution. This approach minimises administrative burden and promotes efficiency by avoiding unnecessary license duplication and associated costs, thereby enabling ministries and agencies to focus resources on strengthening internal data protection mechanisms.

11. CONCLUSION

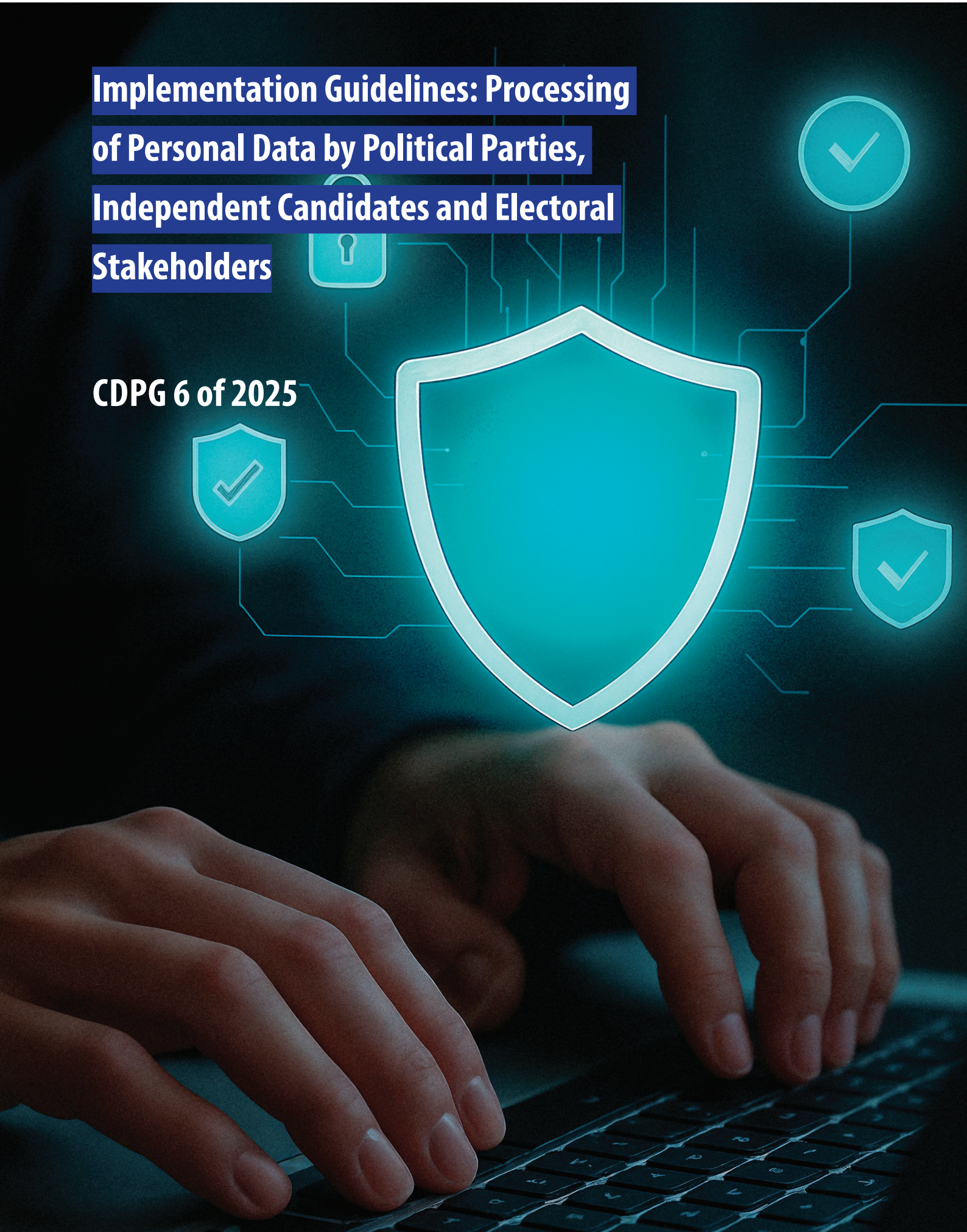
11.1 These guidelines are intended to ensure consistency, legal clarity, and administrative efficiency in the implementation of Zimbabwe's data protection regime within the public sector.

11.2 All MDAs are urged to adhere to these provisions and liaise with POTRAZ for any further clarification.

For further guidance on licensing requirements and process, contact the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) at regulator@potraz.zw or call +263 242 333032/48

Implementation Guidelines: Processing of Personal Data by Political Parties, Independent Candidates and Electoral Stakeholders

CDPG 6 of 2025



Implementation Guidelines: Processing of Personal Data by Political Parties, Independent Candidate and Electoral Stakeholders

1. INTRODUCTION

The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), as the designated Data Protection Authority under section 5 of the Cyber and Data Protection Act, [Chapter 12:07] (hereinafter referred to as "CDPA") is mandated to regulate, promote, and enforce the fair processing of personal data by data controllers in Zimbabwe. The Authority therefore establishes these guidelines to ensure that political parties, their electoral candidates, independent candidates, and electoral stakeholders process personal data lawfully, transparently, and fairly, thereby protecting the rights of citizens and maintaining public trust during and after elections.

2. WHY THESE GUIDELINES?

The Election cycle is data-driven and involves the collection of personal data from voter registration, voter authentication, voting, and results transmission. Electoral candidates rely on data to inform their campaigns, and they determine where to hold rallies and which campaign messages to focus on in specific areas. Electoral processes rely heavily on the collection and use of personal data; therefore, electoral candidates must process personal data lawfully, transparently, and fairly in accordance with the CDPA and S.I 155 of 2024.

3. SCOPE AND PURPOSE

These guidelines are issued in terms of Section 11(3) of the CDPA, which provides that the Authority shall lay down the conditions and circumstances for processing certain categories of sensitive information. By interpretation, membership of a political party and political opinions are classified as sensitive information according to data protection laws in Zimbabwe. Section 20 of the Electoral Act [Chapter 2:13] provides that the voters' roll shall specify, in relation to each registered voter, the voter's first and last names, date of birth, national registration number, and sex; the place where the voter ordinarily resides; and any other information as may be prescribed or as the Commission considers appropriate. In light of the above, these guidelines provide practical advice to all stakeholders involved in electoral processes, including aspiring and elected Members of Parliament, Senators, and Councillors from political parties, as well as independent candidates. It outlines responsibilities, procedures, and safeguards to ensure lawful data processing by aspiring and elected Parliamentarians, Senators, and Councillorss during and after elections.

4. DEFINITIONS OF TERMS

a. Act: Refers to the Cyber and Data Protection Act [Chapter 12:07] of Zimbabwe.

b. Canvassing: refers to the direct engagement with voters by political parties, candidates, or campaign teams to influence voting behaviour, gather support, and promote political messages. It includes activities such as:

i. Door-to-door visits, where canvassers speak with voters, distribute flyers, and record voter preferences or concerns,

ii. Phone banking, where calls are made to voters to discuss issues, encourage participation, or persuade undecided individuals.

iii. Postal canvassing, involving sending election materials to voters using addresses from the voters' roll.

iv. Online canvassing, which includes digital outreach via websites, social media, and targeted advertising.

c. Commission: Refers to the Zimbabwe Electoral Commission (ZEC) established under the Constitution of Zimbabwe.

d. Consent: Any clear, informed, and voluntary agreement by a data subject to the processing of their personal data.

e. Data Controller: A person or entity that determines the purpose and means of processing personal data.

f. Data Processor: A person or entity that processes personal data on behalf of the data controller.

g. Data Protection Authority: means Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ).

h. Data Subject: An individual whose personal data is being processed.

i. Personal Data: Any information relating to an identified or identifiable individual.

j. Political Party: means any political organisation.

k. Sensitive Personal Data: Sensitive Information: refers to personal data that includes biometric data, racial or ethnic origin, political opinions, membership of a political association, and any information that may be considered as presenting a major risk to the rights of the data subject.

l. Processing: Any operation performed on personal data, such as collection, storage, use, deletion, and transfer.

5. REQUIREMENTS FOR PROCESSING OF PERSONAL DATA DURING AND AFTER ELECTIONS

The processing of personal information by aspiring and or elected officials, political parties, and electoral stakeholders, whether during or after electoral processes, constitutes the handling of sensitive data as defined under Section 11 of the CDPA. Such processing is strictly prohibited unless it fully complies with the

specific conditions prescribed by the Act, including obtaining clear, informed consent from the data subject or meeting other lawful grounds for processing as outlined in the Act. Any deviation from these conditions makes the processing unlawful and subject to regulatory enforcement and penalties.

5.1. General Principles

Before processing people's personal information for electoral purposes, the data controller shall:

a. Inform the data subjects of the purpose and

b. obtain consent before processing people's personal data.

5.2. Licensing and Registration

All political parties, the Commission, and independent candidates shall be licensed and register as data controllers before processing personal data of Zimbabweans and shall abide by all the provisions of the CDPA and SI 155 of 2024.

5.3. Appointment of a Data Protection Officer

In line with the provisions of sections 20(5 and 6) and 12 of the CDPA and SI 155 of 2024, respectively, all political parties, independent candidates, and the commission shall appoint a Data Protection Officer

5.4. DATA PROTECTION PRINCIPLES

Political parties and actors increasingly rely on personal data to engage voters. The personal information must be processed lawfully, transparently, and fairly. Therefore, all election candidates shall adhere to the following:

1.1.1 Process data only for the specified use, and the information may not be used for any other purposes.
1.1.2 Collect only necessary personal data for the purpose of elections.
1.1.3 Ensure data is up-to-date and correct.
1.1.4 Keep the data only for as long as necessary.
1.1.5 Make sure that the personal data is protected from unauthorised access, disclosure, alteration, or loss.
1.1.6 Comply with all data protection laws.

6. LAWFUL BASIS FOR PROCESSING PERSONAL DATA

Personal data may only be processed under the following lawful basis:

a. Explicit consent must be sought from the data subject before the processing of personal data. This consent must be freely given, specific, informed, and unambiguous, and must be documented in compliance with the provisions of the Act.
b. All Political parties, independent candidates, the commission, and electoral stakeholders must inform data subjects of their rights, including their right to withdraw consent.
c. The Authority does not recommend the use of legitimate interest as a lawful basis for processing information by Political parties, independent candidates, the commission, and electoral stakeholders.

d. All personal data needs to be processed fairly and lawfully, and in a completely transparent way. In this case, all political parties, their members shall be responsible for informing data subjects of the intention to collect data, how the data will be used, and whether the data is to be shared with other parties, and who the said third party is.
e. Personal data collected must be for a lawful reason and transparent, and it must not be processed in a way that is different from the original purpose.
f. All the personal information collected during and after elections must not be excessive, given the purpose of the collection. Therefore, the personal data should be adequate, relevant, and not excessive.
g. All personal data collected during and after elections must be up to date and accurate, which requires a regular review of data held for the purpose of amending any outdated or inaccurate information. Individuals have the right to have inaccurate data about them erased.
h. Data relating to a data subject must be deleted or anonymised once it has served its purpose, subject to the entity having any other grounds for retaining the information.
i. All political parties collecting or processing data have a responsibility to ensure that reasonable steps have been taken to implement security safeguards. This includes ascertaining the integrity of all employees authorised to access an individual's personal information.
j. Political parties, independent candidates, collecting and/or processing data, must ensure that their practices are compliant with the requirements of processing personal data.

7. DATA SECURITY AND DATA SUBJECTS' RIGHTS

To secure and safeguard personal data being processed, political parties, independent candidates, the commission, electoral stakeholders, or the processor shall:

a. Safeguard the security, integrity, and confidentiality of the data by putting in place appropriate technical and organisational measures that are necessary to protect data from negligent or unauthorised destruction, negligent loss, unauthorised alteration or access, and any other unauthorised processing of the data collected for electoral purposes. Implement privacy by design and by default to ensure that innovation can co-exist with privacy protection in all electoral processes.
b. Restrict physical access to records and supervise access to voter information.
c. Use encryption and password protection when using electronic gadgets.
d. Notify the Data Protection Authority within 24 hours of a breach of personal data being processed.
e. Inform affected individuals within 72 hours if their rights are at risk.
f. Political parties, independent candidates, the commission, electoral stakeholders, or the processor must have robust, real-time mechanisms in place to respond to Data Subject Access Requests (DSARs)

8. SECURING AND SHARING THE VOTER'S ROLL

a. The Electoral Commission must create a secure online portal for accessing the Voter's Roll, ensuring strong access control mechanisms to prevent unauthorized access and maintain security.

b. Any information shared with candidates, particularly the Voter's Roll, must be fully anonymized, adhering strictly to the principle of data minimization and purpose limitation.

9. DUTY TO INFORM DATA SUBJECTS PRIOR TO THE COLLECTION OF THEIR PERSONAL DATA

One of the key principles of data protection is transparency. The personal data processed by political parties, independent candidates, the Commission, and other electoral stakeholders shall be processed fairly and in a transparent manner. They must comply with the obligations under Section 14(1) of the Act, which states that data controllers and data processors have a duty to notify data subjects of the following before the collection of personal data:

a. the rights of the data subject specified under section 14.
b. the fact that personal data is being collected.
c. the purpose for which the personal data is being collected.
d. the third parties whose personal data has been or will be transferred to, including details of safeguards adopted.
e. the contacts of the data controller or data processor, and whether any other entity may receive the collected personal data.
f. a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of the data.
g. the data being collected pursuant to any law and whether such collection is voluntary or mandatory; and
h. the consequences, if any, where the data subject fails to provide all or any part of the requested data.

The above information should be provided to data subjects to enable them to understand how their personal data is used; this can be achieved by a privacy notice. The Authority advises that the information in a privacy notice must be provided in clear, plain language and be provided free of charge. The privacy notice must be kept up to date to meet any changes to the processing of data.

10. DATA COLLECTION AND USE

Aspiring and elected officials shall:

a. Collect only personal data necessary for specific purposes (e.g., political membership, petitions, and grievances).
b. Avoid collecting other sensitive data unless it is necessary and justified.

11. DATA QUALITY AND RETENTION

Political parties, their candidates, and electoral stakeholders shall:

a. Keep data accurate and up to date.

b. Allow the electorate to correct their information.

c. State how long they will keep the data for.

d. Securely delete or anonymize data when no longer needed.

12. TRAINING AND AWARENESS

Political parties, independent candidates, the commission, and related organisations shall:

a. Ensure all electoral stakeholders, including candidates and campaign teams, receive mandatory training on the principles and obligations of data protection under the Act.

b. Promote awareness of data subject rights, including consent, access, correction, and objection to data processing.

c. Educate stakeholders on the definition and handling of personal and sensitive data, especially political opinions, affiliations, and biometric data.

d. Clarify the roles of data controllers and processors, and the requirement to appoint a Data Protection Officer (DPO) where applicable.

e. Emphasize the importance of lawful, fair, and transparent data processing, especially during voter outreach, canvassing, and digital campaigning.

f. Highlight the need for secure data storage and transmission, including protection against unauthorized access, breaches, and cyber threats.

g. Encourage the development and implementation of Data protection policies and internal codes of conduct approved by the Data Protection Authority.

h. Provide guidance on reporting mechanisms for data breaches and non-compliance, including whistleblowing provisions.

i. Reinforce the legal consequences of violating data protection laws, including penalties and reputational risks.

j. Collaborate with the Data Protection Authority to ensure continuous education and compliance monitoring throughout the electoral cycle.

13. ETHICAL CONSIDERATIONS

All people involved in the electoral process must:

a. Respect the dignity and privacy of citizens.

b. Uphold all the rights of data subjects enshrined in the CDPA and CDPR.

c. Do not use personal data for any other purposes separate from the initial purpose.

d. Appoint a Data Protection Officer who shall assist in ensuring compliance with the requirements of processing personal data.

14. PROHIBITED PRACTICES

Processing of information under the following conditions shall be prohibited:

a. Processing data without being licensed and registered as a data controller.

b. Processing and sharing data without consent from data subjects or a legal basis for processing such information.

c. Retaining data indefinitely without justification.

d. Transferring and sharing collected information for the purpose of elections outside Zimbabwe.

15. PENALTIES AND FINES FOR NON-COMPLIANCE

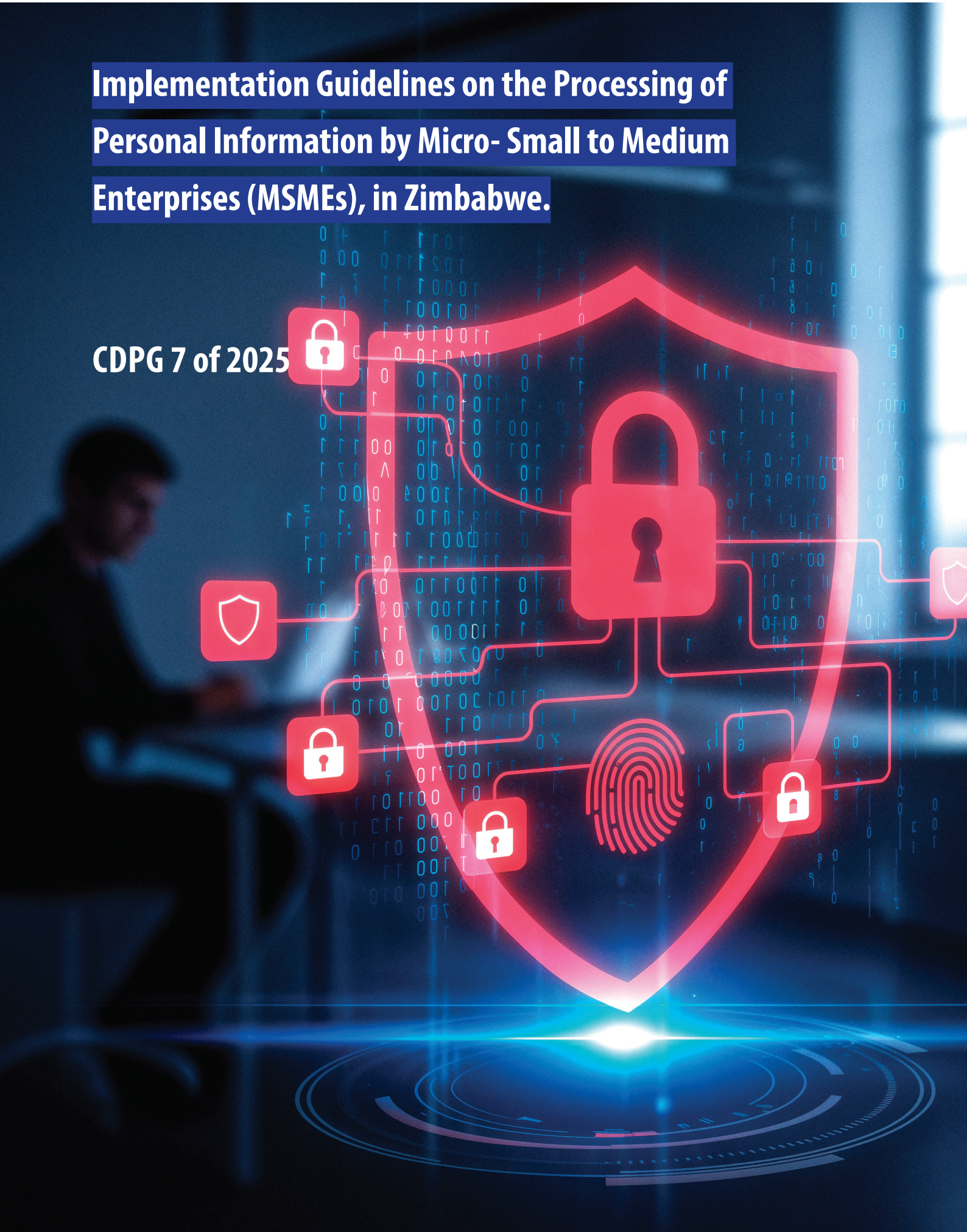
Any person who does not comply with the provisions of the Cyber and Data Protection Act and SI 155 of 2024 shall be liable for the following fines and penalties:

a. Fines up to level 11 for processing personal data without a valid data controller license, as well as breaching the provisions of the Act and the Regulations.
b. Imprisonment of up to 7 years for the same offence
c. License Cancellation, which renders the processing of personal data unlawful.

For complaints and further guidance, contact the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) at regulator@potraz, gov.zw or call +263 242 333032/46/48.

Implementation Guidelines on the Processing of Personal Information by Micro- Small to Medium Enterprises (MSMEs), in Zimbabwe.

CDPG 7 of 2025



Implementation Guidelines on the Processing of Personal Information By Micro- Small To Medium Enterprises (MSMEs), in Zimbabwe.

1. PURPOSE AND EFFECTIVE DATE

These guidelines are issued in accordance with section 6 of the Cyber and Data Protection Act [Chapter 12:07] (hereinafter referred to as "the CDPA"), which mandates the Authority to produce regulatory sectoral guidelines to facilitate and promote the fair processing of personal data in Zimbabwe. These guidelines seek to assist data controllers within the MSMEs sector to fully understand the application scope of the CDPA and effectively aid understanding of their respective compliance obligations. The guidelines shall be read in conjunction with the provisions of the CDPA and Section 11 of Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations, 2024 (SI 155 of 2024). The Guidelines shall be effective from the date of publication.

2. INTERPRETATION

In these Guidelines, the following shall mean:

"CDPA" refers to the Cyber and Data Protection Act [Chapter 12:07]

"Data Protection Authority (DPA) or "the Authority" refers to the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), designated as such in terms of section 5 of the Cyber and Data Protection Act.

"Data Controller" refers to any natural person or legal person who is licensable by the Authority, including public bodies and any other person who determines the purpose and means of processing personal data.

"Data protection officer" or "DPO" refers to any individual appointed by the data controller and who is charged with ensuring, in an independent manner, compliance with the obligations provided for in the CDPA.

"Personal information" means information relating to a data subject which can be used to identify an individual.

"Processing" refers to any operation or set of operations that are performed upon data, whether or not by automatic means, such as obtaining, recording or holding the data or carrying out any operation or set of operations on data.

"Data Subject" means an identified or identifiable natural person who is the subject of data.

"Sensitive data" refers to information or any opinion about an individual which reveals or contains, racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sex life; criminal, educational, financial or employment history; gender, age, marital status or family status.

"Cross-border transfer of data" refers to the transfer of personal data beyond the borders of Zimbabwe.

"SME Act" refers to the Small to Medium Enterprises Act [Chapter 24:12]

"Micro- small to medium enterprises" refers to a business, either incorporated or not, run by one or more people, with or without branches or subsidiaries, that mainly operates in a specific sector of the economy of Zimbabwe.

SCOPE AND APPLICATION

These guidelines apply to the processing of personal data by MSMEs. They seek to provide a clear understanding of MSMEs' obligations under the Cyber and Data Protection Act [Chapter 12:07]. They present a simplified approach to assist MSMEs in understanding the scope of their data processing activities, including the collection, use, retention, disclosure, and disposal of personal data, which incline to recommended data protection practices. These guidelines apply to all MSMEs established or ordinarily resident in Zimbabwe in terms of the Small to Medium Enterprises Act [Chapter 24:12], as read with section 4 (2) (b) of the CDPA.

3. BACKGROUND

Most business operations involve the processing of personal data. MSMEs collect personal data, and they must process data in a lawful, transparent and fair manner, ensuring that they implement all data protection principles in their processing activities to comply with the CDPA.

3. ARE ORGANISATIONS IN THE MSMEs SECTOR DATA CONTROLLERS IN TERMS OF THE CDPA?

3.1. According to section 3 of the CDPA, a data controller refers to any natural or legal person who is licensable by the Authority, including public bodies and any other person who determines the purpose and means of processing personal data.

3.2. Additionally, section 3 of SI 155 further clarifies that a person must obtain a license if they process personal data with any of the following intentions:

- Determining the means, purpose, or outcome of data processing.
- Deciding what personal data to collect.
- Selecting the individuals from whom to collect data.
- Using personal data for commercial gain or other benefits

3.3. From the definition, MSMEs are data controllers.

4. ARE MSMEs LICENSED BY THE AUTHORITY AS DATA CONTROLLERS?

4.1. Any person who processes personal information for more than 50 data subjects is licensable by the Authority.

4.2. Classes of MSMEs

- Micro enterprises

Micro enterprises are typically very small entities, often informal and operated by a sole trader or a partnership of two individuals.

In Zimbabwe, licensing and registration are required for organisations that process personal information for 50 and above data subjects.

Micro enterprises must carefully assess whether they process information for more than 50

data subjects.

If a micro-enterprise processes information for fewer than 50 data subjects, it is not required to apply for a data controller licence.

However, it must still comply with the data protection principles set out in the Cyber and Data Protection Act and its Regulations.

Small enterprises

Small enterprises are basically very small in size but generally larger than micro enterprises. They are formally structured and are either run by a sole trader or more people and typically employ more employees than micro enterprises.

In Zimbabwe, licensing and registration are required for organisations that process personal information for 50 and above data subjects.

In that regard, small enterprises must also carefully assess whether they process information for more than 50 data subjects.

If they process personal information for less than 50 data subjects, they are not required to apply for a data controller licence.

However, they must still comply with the data protection principles set out in the Cyber and Data Protection Act and its regulations.

- Medium enterprises

Medium enterprises are formally registered businesses that are larger than small enterprises but not as big as a large corporation. They typically employ more people than small enterprises, and they operate in different sectors of
of the economy.

Most medium-sized enterprises process personal information for more than 50 data subjects.

Some are likely to fall within tier 1, with others slightly falling into tier 2, and if that is the case, they are required to register and apply for a license, in compliance with the Data Protection laws.

In Zimbabwe, organisations are categorised into tiers for data protection licensing purposes and the type of data controller licence an organisation needs is based on the number of people whose personal data it processes, and not the number of employees

4.3. See the definition of tiers below

- MSMEs that process personal information for 50- 1000 data subjects fall under tier 1.
- MSMEs that process personal information for 1001 to 100,000 data subjects fall under tier 2.

5. ARE ORGANISATIONS WITHIN THE MSME COMMUNITY MANDATED TO APPOINT A DATA PROTECTION OFFICER?

5.1. Any MSME that processes personal data subjects that are above 1000 are mandated to appoint a DPO.

5.2. Any MSME with 50 and above data subjects that processes sensitive information is also required to appoint a DPO.

6. APPLICATION OF DATA PROTECTION PRINCIPLES BY MSMEs

6.1. MSMEs must process data in a lawful, transparent and fair manner as enshrined in the law.

6.1.1. This entails that:

- All MSMEs should seek consent from the data subject before processing data.
- Consent shall be in writing for the processing of sensitive personal data, or for the transfer of personal data outside of Zimbabwe
- MSMEs can process personal data for a clear, known legitimate interest of the business, e.g. Human Resources Management, security reasons.
- MSMEs can also process data lawfully to fulfil obligations from a contractual agreement between themselves and other parties.
- It is also lawful for MSMEs to process personal data if the processing is in the vital interests of the data subject, e.g. in case of health emergencies where processing is necessary to save or protect a data subject's life.

6.2. In the processing of personal data, MSMEs must ensure that:

- Personal data is processed for the purpose for which it was collected and it is prohibited to process data for another purpose that was not specified.
- Personal information is not kept for more than necessary in relation to the purposes for which it was collected.
- Personal data kept by MSMEs must be correct and up to date.
- They demonstrate compliance with all data protection principles and all obligations outlined in the CDPA and the Regulations-(SI 155 of 2024).
- All MSMEs are accountable to the DPA to follow the law.

6.3. Simple Self-assessment Strategies for MSMEs to Implement Data Protection Principles

It is encouraged that MSMEs conduct an evaluation to determine the following;

- The type of data they process
- Why they need to store that data, for example, for tax reasons
- How and where the data will be stored securely, either by the business or a third-party organisation
- How the data can be accessed by data subjects if needed
- Periods they need to keep the data
- How the data is deleted or destroyed

7. RISKS THAT MSMEs SHOULD LOOK OUT FOR IN THE PROCESSING OF PERSONAL DATA

7.1. Unauthorised Access

- Storing data manually can be easier to access without proper authorisation, leading to breaches of privacy of sensitive information falling into the wrong hands.

7.2. Human Error

- Manual processes can be prone to human error, including misfiling documents,
- Lack of or no verification of information, and unintentional disclosure of information can lead to inaccurate processing of data.

7.3. Excessive storage

Lack of defined periods of keeping personal data can lead to storage of large volumes of unnecessary personal information, which in turn;

- Create more entry points for cyberattacks/ increased cyber threats
- Makes it harder to secure all data effectively.
- Increase the risk and impact of a breach, especially if sensitive data is involved.

8. INSTANCES OF NON-COMPLIANCE TO WATCH OUT FOR

8.1. Processing personal data without a license.
8.2. Failure to appoint a data protection officer.
8.3. Processing children's personal information without the authority of their parent or guardian.
8.4. Failure to report a data breach after being aware of such breach to the Authority within 24 hours and within 72 hours to the affected data subjects.
8.5. Providing false information to the Authority
8.6. Failure to renew a data protection licence.
8.7. Processing and transferring personal data outside of Zimbabwe without approval from the Authority.

9. PENALTIES AND FINES FOR NOT FOLLOWING THE LAW

Failure to follow the law will result in the following;

a) Fines up to level 11,

b) Imprisonment up to 7 years

c) An order to stop the processing of personal data- (Cancellation of Data Protection License.)

10. PRACTICAL RECOMMENDATIONS AND TIPS FOR MSMEs WHEN PROCESSING PERSONAL INFORMATION

MSMEs should;

- Seek professional guidance and advice from the Authority
- Appoint or train a certified DPO
- Establish a clear reason relevant to the business for processing personal data
- Create clear ways to seek consent from data subjects and to

establish a communication framework in a way that respects data subject's rights, e.g, consent forms, privacy notices, etc

- Use encryption, password protection, and secure cloud services as part of the technical measures to secure the integrity and confidentiality of personal data.

- Restrict physical access to records and supervise visitors
- Invest in data protection awareness and capacity building for staff, as part of existing capacity building initiatives
- implement storage mechanisms that ensure that they keep personally identifiable information for no longer than necessary
- Set up clearly defined procedures for secure deletion of personal data.
- Strive to get awareness of stipulated legal retention limits for different data types and sectors (e.g. financial and health data)

ANNEXURE 1: COMPLIANCE CHECKLIST FOR MSMEs

Description of requirement	YES	NO	Comments
Data controller licence			
If tier 2 and above- Appointment of a DPO			
A recognised reason for processing personal data			
Training and awareness			
Implementation of Data protection principles			
Records of all Processing Activities			
Consent forms/ data subjects access request forms			
Data Protection Policy/ Privacy policies			
Periods of keeping data			
Approval for transfer of Data outside of Zimbabwe			
Data processing/ sharing agreements in place with processors			
Data Protection Impact Assessments when necessary (Transfer of data outside Zimbabwe, integration of new technologies, data processing using digital means, processing sensitive data, children's data)			
Measures to ensure the security and confidentiality of data			
Risk assessments and reports			
Valid consent- processing of children's data			

For compliance and further guidance, contact the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) at regulator@potraz.zw or call +263 242 333032/48

1110 Perfomance Close, Mt Pleasant Business Park
P.O Box MP 843, Mt Pleasant,
Harare, Zimbabwe

Toll Free Number: 0800 4303
Tel: +263 24-2-333032
Fax: +263 24-2-333041

