



CONSULTATION PAPER ON THE INTRODUCTION OF ADMINISTRATIVE PENALTIES FOR NON-COMPLIANCE WITH DATA PROTECTION REQUIREMENTS UNDER THE CYBER AND DATA PROTECTION ACT [CHAPTER 12:07]

1. INTRODUCTION

- 1.1. The protection of personal information is increasingly important in Zimbabwe's rapidly digitising economy and strengthening of data protection and cybersecurity is a key priority of the Government of Zimbabwe¹. Organisations across both the public and private sectors collect, process, store, share and transfer large amounts of personal information. The Cyber and Data Protection Act² establishes the legal framework for the protection of personal information and designates the Postal and Telecommunications Regulatory Authority of Zimbabwe³ (POTRAZ) as the Data Protection Authority⁴ (hereinafter referred to as 'the Authority').
- 1.2. Since the commencement of the data protection framework, significant progress has been made in building awareness, developing institutional capacity, licensing data controllers and encouraging organisations to establish data protection governance structures.
- 1.3. As the data protection ecosystem matures, the need to strengthen the Authority's enforcement toolkit cannot be overemphasized. One mechanism under consideration in this paper is the introduction of administrative penalties for specified instances of non-compliance. Currently, the law provides for criminal sanctions only in section 33 of the Act and in specific provisions in the regulations⁵.
- 1.4. The Authority proposes to amend the existing licensing regulations to incorporate provisions that speak to administrative penalties and the procedural

¹ National Development Strategy 2

² [Chapter 12:07]

³ Established in terms of section 4 of the Postal and Telecommunications Act [Chapter 12:05]

⁴ Section 5 of the Cyber and Data Protection Act [Chapter 12:07]

⁵ Statutory Instrument 155 of 2024

processes for the imposition of such fines rather than developing a new set of regulations on administrative penalties.

- 1.5. This Consultation Paper seeks the views of stakeholders on the proposed framework, principles, procedures and safeguards for imposing administrative penalties.

2. PURPOSE OF THE CONSULTATION

The specific purpose of this consultation is to obtain stakeholder views on:

- 2.1. the nature of administrative penalties that should be introduced as an additional data protection enforcement mechanism.
- 2.2. the types of contraventions that should attract administrative penalties.
- 2.3. the appropriate methodology for determining the amount of a penalty.
- 2.4. factors that should aggravate or mitigate a penalty.
- 2.5. procedural safeguards that should apply before a penalty is imposed.
- 2.6. the relationship between administrative penalties and criminal sanctions.
- 2.7. the type of breaches that attract compensation of data subjects.
- 2.8. appropriate treatment of public bodies, small organisations and other entities with limited resources.
- 2.9. mechanisms for review, appeal and enforcement of administrative penalty decisions.

3. CURRENT ENFORCEMENT TOOLKIT

- 3.1. The Cyber and Data Protection Act establishes conditions and obligations relating to the lawful processing⁶ and protection of personal information and provides the Data Protection Authority with specific functions in section 6 of the Act. Among many other functions, the Authority is empowered to conduct inquiries⁷ and investigations, receive and investigate complaints⁸ and promote and enforce⁹ fair processing of personal information in accordance with the Act.
- 3.2. The Act and the Regulations¹⁰ also outlines criminal sanctions for specified contraventions. Section 33, for example, provides for certain contravention that constitute offences punishable upon conviction by a court. Convicted offenders may be liable to a fine not exceeding level 7¹¹ or 11¹² or imprisonment for a period not exceeding seven (7) years or to both such fine and imprisonment.
- 3.3. However, the Authority has noted that reliance solely on criminal proceedings may not provide a sufficiently flexible, proportionate or timely response to the full range of regulatory non-compliance that characterises the data protection ecosystem. It is the considered view of the Authority that administrative

⁶ Section 6 (1) (a)

⁷ Section 6 (1) (f)

⁸ Section 6 (1) (g) (h)

⁹ Section 6 (1) (b)

¹⁰ Statutory Instrument 155 of 2024

¹¹ Section 33 (1)

¹² Section 33 (2)

penalties can provide an intermediate enforcement mechanism between regulatory engagement and criminal prosecution.

- 3.4. In addition, reliance on criminal sanctions alone exerts an unnecessary burden on the criminal justice system considering the magnitude of the ecosystem that is regulated by the Authority in terms of data protection compliance.

4. WHY INTRODUCE ADMINISTRATIVE PENALTIES?

Administrative penalties are monetary penalties assessed and imposed by a regulator without recourse to a court or independent administrative tribunal. The Australian Law Reform Commission defined administrative penalties as “*sanctions imposed by the regulator, or by the regulator’s enforcement of legislation, without intervention by a court or tribunal.*”¹³ The proposed administrative penalties framework under Zimbabwean law is intended to address the regulatory objectives listed below.

4.1. Strengthening compliance

Administrative penalties create a credible consequence for persistent or serious non-compliance and can encourage organisations to take data protection obligations seriously.

4.2. Proportional enforcement

Not every contravention warrants criminal prosecution. Administrative penalties would enable the Authority to distinguish between:

- (i) minor administrative deficiencies.
- (ii) negligent non-compliance.
- (iii) repeated non-compliance.
- (iv) serious violations; and
- (v) deliberate or reckless violations.

4.3. Timely regulatory intervention

An administrative mechanism can provide a more efficient regulatory response than relying exclusively on criminal proceedings.

4.4. Promoting accountability

The objective should not simply be to punish organisations. Penalties should reinforce the principle that organisations processing personal information must be able to demonstrate accountability and responsible data governance.

4.5. Compensation of data subjects

Ultimately, effective enforcement should contribute to reducing harm to individuals and strengthening public confidence in the digital economy. Currently, the law does not provide for compensation for data subjects in cases of data breaches unlike in other countries such as Tanzania which have provisions for compensating data subjects.

¹³ ALRC, Principled Regulation: Federal Civil and Administrative Penalties in Australia (Final Report), March 2003

5. REGIONAL BENCHMARKING

The Authority's proposal to introduce administrative fines is also informed by regional and international good practice. A scan of other legal and regulatory frameworks on data protection indicated the existence of both administrative and criminal sanctions as complementary enforcement tools for regulators.

Table 1: Regional comparative schedule of fines

Country	Governing Law	Regulator	Maximum Administrative Fine	Criminal Penalties	Currency Note (approx. USD)
Kenya	Data Protection Act, 2019 (No. 24 of 2019)	Office of the Data Protection Commissioner (ODPC)	Up to KES 5,000,000, or up to 1% of annual turnover of the preceding financial year, whichever is lower	General offence: fine up to KES 3,000,000 and/or imprisonment up to 10 years (may be imposed in addition to or as alternative to the fine)	≈ USD 35,000 (max admin fine)
Eswatini	Data Protection Act, 2022 (Act No. 5 of 2022)	Eswatini Communications Commission (ESCCOM)	Administrative fine: up to E5,000,000 or up to 2% of annual turnover Serious/criminal offences: up to E100,000,000 or up to 5% of annual turnover	Imprisonment up to 10 years for serious offences (may apply to the head of a juristic-person data controller)	≈ USD 268,000 (admin) / ≈ USD 5.5M (serious offences)
Botswana	Data Protection Act, 2024 (repeals the 2018 Act; effective January 2025)	Information and Data Protection Commission	Maximum administrative fine: BWP 50,000,000 (raised from BWP 10,000,000 under the repealed 2018 Act)	Fines and imprisonment for specific offences under the prior regime ranged BWP 100,000–1,000,000 with imprisonment terms of 3–12 years; the 2024	≈ USD 3,685,000 (max admin fine)

Country	Governing Law	Regulator	Maximum Administrative Fine	Criminal Penalties	Currency Note (approx. USD)
				Act carries comparable custodial sanctions	
Malawi	Data Protection Act, 2024 (Act No. 3 of 2024)	Malawi Communications Regulatory Authority (MACRA) / Data Protection Authority	Regulatory offence fine: up to MWK 5,000,000	Imprisonment up to 12 months (may apply in addition to the fine, per regulations under the Act)	≈ USD 2,900 (max fine, indicative)
Zambia	Data Protection Act, 2021 (Act No. 3 of 2021)	Data Protection Commissioner / Data Protection Commission	Body corporate: 600,000 Kwacha, or 2% of annual turnover, whichever is higher Natural person: up to 300,000 Kwacha Registration offences: up to 500,000 penalty units General offence (no specified penalty): up to 300,000 penalty units	Natural person: imprisonment up to 10 years General/registrarion offences: imprisonment up to 3–5 years (fine and imprisonment may both apply)	≈ USD 26,658 (body corporate) / ≈ USD 13,329 (individual)
South Africa	Protection of Personal Information Act, 2013 (POPIA,	Information Regulator	Administrative fine: up to ZAR 10,000,000	Serious offences: fine and/or imprisonment up to 10 years Minor offences: fine and/or	≈ USD 545,000 (max admin fine)

Country	Governing Law	Regulator	Maximum Administrative Fine	Criminal Penalties	Currency Note (approx. USD)
	in force 2021)			imprisonment up to 12 months	

6. REGULATORY PRINCIPLES

The Authority also proposes several regulatory principles to support the implementation of the proposed administrative penalty framework. The principles are meant to not only bring certainty but ensure that regulatory action is transparent and fair. The following principles will guide the work of the Authority in implementing administrative penalties:

6.1 Legality

No administrative penalty shall be imposed unless there is a clear legal basis for doing so.

6.2 Proportionality

The penalty shall correspond to the seriousness of the contravention and the circumstances of the case.

6.3 Consistency

Similar cases shall, as far as reasonably possible, result in comparable enforcement outcomes.

6.4 Fairness

Affected organisations shall be given a reasonable opportunity to respond to allegations before a final decision is made.

6.5 Transparency

The methodology used to determine penalties shall be published and understandable.

6.6 Accountability

The Authority shall maintain appropriate records of enforcement decisions and periodically report on enforcement activity.

6.7 Corrective regulation

Where appropriate, penalties shall be accompanied by corrective measures designed to bring an organisation into compliance.

6.8 Deterrence

Penalties shall be sufficiently meaningful to discourage deliberate, reckless or persistent non-compliance.

7. PROPOSED CATEGORIES OF CONTRAVENTIONS

It is also imperative to solicit view of stakeholders on the categories of contraventions that should attract an administrative penalty. The following categories are for consideration and comments by stakeholders.

7.1. Category A: Regulatory and administrative non-compliance

Examples may include:

- (a) failure to maintain required registration or licensing.
- (b) failure to appoint a Data Protection Officer where required.
- (c) failure to maintain prescribed records.
- (d) failure to cooperate with a lawful regulatory request.
- (e) failure to submit required information to the Authority; and
- (f) failure to comply with regulatory directions.

7.2. Category B: Governance failures

Examples may include:

- (a) failure to implement appropriate data protection policies.
- (b) failure to establish appropriate accountability mechanisms.
- (c) failure to conduct required risk assessments or Data Protection Impact Assessments.
- (d) failure to provide adequate training; and
- (e) failure to appropriately supervise persons processing personal information.

7.3. Category C: Individual rights violations

Examples may include:

- (a) unjustified refusal to respond to a data subject request.
- (b) unreasonable delay in responding to a request.
- (c) failure to provide required information to data subjects; and
- (d) unlawful processing of personal information.

7.4. Category D: Security and breach-related failures

Examples may include:

- (a) failure to implement appropriate technical and organisational safeguards.
- (b) failure to adequately manage known security risks.
- (c) failure to notify the Authority or affected persons where legally required; and
- (d) failure to take reasonable steps to mitigate harm following a personal data breach.

7.5. Category E: Serious violations

More serious violations could include:

- (a) intentional unlawful processing.
- (b) Unlawful processing of personal data of vulnerable groups (e.g children)
- (c) deliberate disclosure of personal information.
- (d) repeated violations following regulatory intervention.
- (e) processing that causes significant harm to data subjects; and
- (f) obstruction of a regulatory investigation.

8. AGGRAVATING FACTORS

The Authority also seeks the views of stakeholders on factors that may be considered as aggravating factors justifying an increased penalty. The following are proposed for consideration and comments by stakeholders:

- 8.1. intentional violation.
- 8.2. deliberate concealment of a violation.
- 8.3. repeated non-compliance.
- 8.4. failure to cooperate with the Authority.
- 8.5. obstruction of an investigation.
- 8.6. significant numbers of affected data subjects.
- 8.7. involvement of sensitive personal information.
- 8.8. substantial financial or other harm.
- 8.9. obtaining commercial benefit from the violation; and
- 8.10. failure to implement corrective measures following previous regulatory intervention.

9. MITIGATING FACTORS

The Authority also submits the following factors to justify a reduction in the penalty for comments by stakeholders:

- 9.1. prompt voluntary disclosure.
- 9.2. immediate remedial action.
- 9.3. effective cooperation with the Authority.
- 9.4. absence of previous violations.
- 9.5. demonstrable compliance programme.
- 9.6. effective incident response.
- 9.7. limited duration of the violation.
- 9.8. absence of actual harm.
- 9.9. reasonable steps taken to prevent the violation; and
- 9.10. circumstances beyond the organisation's reasonable control.

10. ADMINISTRATIVE PENALTIES AND CRIMINAL SANCTIONS

A critical issue for consultation is the relationship between administrative penalties and criminal proceedings. Stakeholders are being called upon to comment on when a matter should be dealt with administratively and when it should be referred for criminal prosecution. While administrative penalties should generally be appropriate for regulatory non-compliance where an administrative response is sufficient, serious, deliberate or criminal conduct may warrant referral to the appropriate law-enforcement or prosecutorial authorities. The Authority proposes that where an administrative penalty has been proposed, criminal sanctions should be dropped

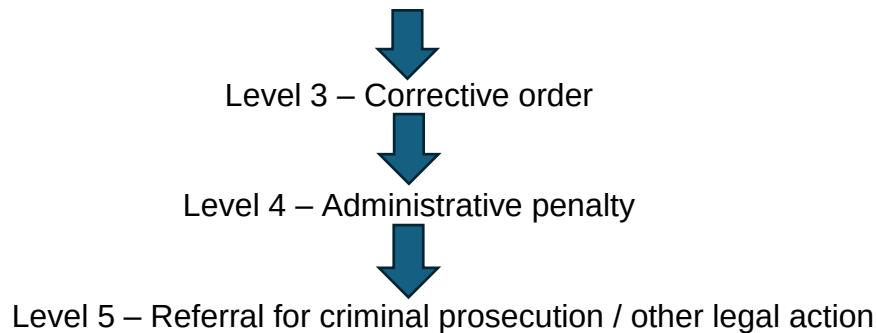
11. SHOULD THERE BE A WARNING BEFORE A PENALTY?

The Authority proposes a graduated approach to enforcement as follows for consideration and comment by stakeholders.

Level 1 – Guidance and education



Level 2 – Non-Compliance notice



However, the Authority retains discretion to move directly to a higher level where the seriousness, intentionality or potential harm of the conduct warrants immediate action.

12. SPECIAL CONSIDERATION FOR SMEs AND PUBLIC BODIES

The Authority recognises that organisations in the Zimbabwean ecosystem differ considerably in size, resources and processing activities. It is the proposal of the Authority that Small and medium-sized enterprises should not necessarily be subjected to the same monetary penalties as large corporations for equivalent conduct where their circumstances materially differ. At the same time, an organisation should not be able to avoid meaningful enforcement merely because it is small.

For public bodies, the Authority proposes that the enforcement should consider the public interest and the need to ensure that government institutions meet the same high standards of accountability expected of private-sector organisations.

In consideration of different data controllers, small and large corporations, stakeholders are invited to comment on whether penalties should be structured using:

12.1. Option A: Fixed penalties

Specified contraventions to attract predetermined penalty amounts for certainty and simplicity considering the differences in organisational size, harm or circumstances.

12.2. Option B: Percentage-based penalties

Penalties are calculated by reference to an organisation's turnover or another appropriate financial measure.

12.3. Option C: Tiered penalties

Contraventions are categorised according to seriousness, with minimum and maximum amounts prescribed for each category for consistency and flexibility.

12.4. Option D: Hybrid model

A combination of fixed, tiered and proportionate penalties depending on the nature of the contravention. The Authority proposes that stakeholders consider a hybrid or tiered model as a possible approach.

13. PUBLICATION OF ENFORCEMENT DECISIONS

The Authority proposes publishing selected enforcement decisions to promote transparency and regulatory consistency. It is proposed that published decisions contain:

- (i) nature of the violation.
- (ii) sector.
- (iii) regulatory provisions involved.
- (iv) factors considered.
- (v) penalty imposed; and
- (vi) corrective action required.

Personal information that is not necessary for regulatory transparency should be redacted. Publication would also allow organisations to learn from enforcement decisions and improve their own compliance programmes.

14. OFFENCES AND FINES RELATING TO DATA PROTECTION OFFICERS

Currently there are no administrative or criminal sanctions attached to offenses that may be committed by Data Protection Officers in the course of discharging their duties. The Authority proposes that offenses and penalties should extend to unlawful conduct by Data Protection Officers.

15. QUESTIONS FOR STAKEHOLDERS

Stakeholders are invited to provide views on the following questions:

- 15.1. Do you support the introduction of administrative penalties for data protection non-compliance in Zimbabwe?
- 15.2. Which categories of non-compliance should attract administrative penalties?
- 15.3. What should be the maximum administrative penalty?
- 15.4. Should penalties be fixed, tiered, percentage-based or hybrid?
- 15.5. What factors should be considered when determining the amount of a penalty?
- 15.6. Should the size and financial capacity of an organisation be considered?
- 15.7. Should first-time offenders generally receive a warning?
- 15.8. In what circumstances should the Authority impose an immediate penalty?
- 15.9. What procedural safeguards should apply?
- 15.10. How should administrative penalties interact with criminal sanctions?
- 15.11. How should public bodies be treated?
- 15.12. How should SMEs and organisations with limited resources be treated?
- 15.13. Should enforcement decisions be published?
- 15.14. What additional safeguards should be included to ensure fairness, transparency and consistency?
- 15.15. Should the Authority issue compensation orders in favour of data subjects and in what circumstances?
- 15.16. Should the Authority prescribe offenses relating to the conduct of Data Protection Officers and what conduct should be penalised?

16. CONCLUSION

- 16.1. Zimbabwe has made significant progress in establishing the foundations of a national data protection framework. The next stage is to ensure that the regulatory system has an enforcement architecture capable of promoting sustained compliance while remaining fair, proportionate and transparent.

- 16.2. The introduction of administrative penalties should therefore be viewed not simply as the creation of another sanction, but as part of a broader graduated enforcement framework. The ultimate objective is not to punish organisations. It is to create a regulatory environment in which organisations understand that responsible processing of personal information is a fundamental governance obligation; data subjects have meaningful protection; and organisations that demonstrate genuine accountability are treated differently from those that deliberately or repeatedly disregard their obligations.
- 16.3. The Authority therefore invites stakeholders to participate actively in this consultation and help shape an administrative penalty framework that is effective, proportionate, predictable, transparent and appropriate to Zimbabwe's data protection ecosystem.
- 16.4. To expedite the consultation process, the Authority has prepared preliminary draft regulations for consideration and comments.

17. SUBMISSION OF COMMENTS

Stakeholders are invited to submit written comments on this Consultation Paper in general and also complete the Consultation Questionnaire by the 30 November 2026.

17.1. The Authority particularly welcomes submissions from:

- (i) data controllers.
- (ii) data processors.
- (iii) Data Protection Officers.
- (iv) data subjects and consumer organisations.
- (v) government ministries and departments.
- (vi) professional bodies and associations.
- (vii) civil society organisations.
- (viii) academia; and
- (ix) other interested stakeholders.

17.2. Comments can be submitted to:

The Director General

POTRAZ

1110 Performance Close

Mount Pleasant Business Park

Harare

Or emailed to consultation2026@dpa.zw