



CLIENT AWARENESS BOOKLET · OCTOBER 2026

Data Protection starts with trust.

A plain-language guide to Zimbabwe's Cyber and Data Protection Act and SI 155 of 2024: what the law asks of your organisation, and why now is the time to act.

ENFORCEMENT HAS STARTED

**POTRAZ began mandatory data
protection inspections on 1 September
2026.**

Is your organisation ready?

www.berachah.global

ZIMBABWE

Unit 4, 25 Shortheath Road, Chisipite, Harare, Zimbabwe

+263 777 762 769 · info@berachah.global

Awareness only. Not legal advice. Verify current requirements.



Enforcement Has Started

Zimbabwe's data protection law is not new. The compliance deadlines have passed, and POTRAZ, the Data Protection Authority, has moved from awareness to inspection.

2021

Cyber and Data Protection Act [Chapter 12:07] enacted. POTRAZ named the Data Protection Authority.¹

13 Sep 2024

SI 155 of 2024 in force: licensing of data controllers and appointment of DPOs.²

12 Dec 2024

Deadline for existing data controllers to appoint a DPO (90 days after SI 155).²

12 Mar 2025

Deadline for existing data controllers to hold a licence (six months after SI 155).²

Mar 2026

Regulatory Notice 1 of 2026 warns unlicensed organisations of enforcement action.⁵

1 Sep 2026

Mandatory compliance inspections begin under Regulatory Notice 2 of 2026.

Who is first in line?

Inspections are risk-based. Banks and financial institutions, insurers, local authorities and healthcare providers come first, followed by mines, religious organisations, schools and colleges, professional bodies, government ministries and agencies, and NGOs.⁴

The Law, In Plain Terms

The Act

The Cyber and Data Protection Act [Chapter 12:07] sets the rules, gives people rights, creates offences and names POTRAZ as regulator.¹

SI 155 of 2024

The regulations that put the Act to work: licensing, DPO appointments, security and breach reporting.²

Key words

Personal information

Anything that identifies a living person (the “data subject”): name, phone, address, ID number, photo, fingerprints, school, work or health details, online identifiers.

Sensitive data

Extra-private information, such as race, political views, religion, trade union membership, sex life, health, genetic and biometric data, and criminal, financial or employment history.

Data controller

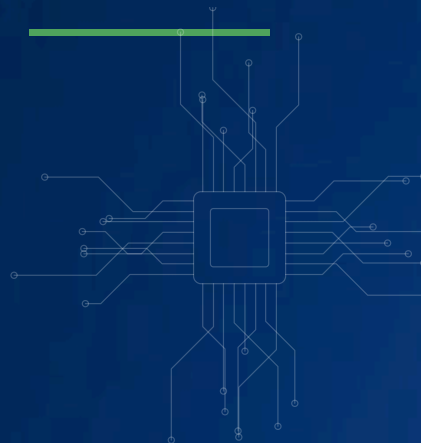
The organisation that decides why and how data is used. This is who needs the licence.

Data processor

An outside party handling data for the controller, such as a payroll, IT or cloud provider.

Processing

Almost anything done with data: collecting, storing, using, sharing, changing or deleting it. Paper records count too.



Does This **Apply To Us?**



You are a data controller if you decide what personal data to collect, whose data to collect and how it is used, or if you use personal data for commercial gain.² That includes companies, schools, clinics, churches, NGOs, councils and ministries.

50+

people whose data you process means a licence.²
Count people, not staff: customers, patients, learners, members, suppliers' contacts and employees all count.

Points people **often miss**

Fewer than 50 people?

POTRAZ's guidance for micro and small enterprises says you need not apply for a licence, but you must still follow the rules.³

Paper counts.

Registers, files, forms and visitor books are personal data too, and inspectors check them.

It is not only an IT issue.

HR files, CCTV, WhatsApp groups and membership lists are all in scope.

Limited exemptions

Purely personal or household use, and some law enforcement, journalistic, historical and archival work, may be exempt from licensing. The data protection principles still apply, so have any exemption assessed before relying on it.²



The Data Controller Licence



Your tier depends on how many people's personal data you process.²

Tier	Data subjects	Annual fee	Application fee
1	50 to 1,000	USD 50	None
2	1,001 to 100,000	USD 300	USD 30
3	100,001 to 500,000	USD 500	USD 30
4	Over 500,000	USD 2,500	USD 30

Fees from SI 155, Second Schedule.² Confirm current fees and any VAT with POTRAZ before applying.

How it works

- Apply on **Form DP1**. POTRAZ must respond within **14 days**.²
- Tell POTRAZ if you process **biometric or genetic data**, such as fingerprint clock-ins or facial recognition.²
- A licence lasts **12 months**. Apply to renew at least **3 months before expiry**; failing to renew is an offence.²
- Existing organisations had until **12 March 2025**. Still unlicensed? Make this your first step.²

The Data Protection Officer

05 · THE DPO

SI 155 requires data controllers to appoint a Data Protection Officer and notify POTRAZ on **Form DP2**.² Assess this separately from licensing.

When smaller enterprises need one³

1,000+

people's data held

50+

people's sensitive data held

These are triggers named in POTRAZ's guidance for micro, small and medium enterprises. Staff files often hold health, financial and family details, so many employers meet the sensitive-data trigger.

What a DPO must have

- 1 Skills, qualifications or experience in law, audit, information security, data science or a related field.²
- 2 Knowledge of Zimbabwe's data protection law, and an understanding of your organisation's operations.²
- 3 A **POTRAZ-approved certification**, kept current every year.^{2,3}





What A DPO Does

Monitors compliance	Trains staff	Runs internal audits
Advises on impact assessments	Handles POTRAZ requests	Contact point for the public

The law expects the DPO to ensure compliance independently.^{1,2}

ADMIN DEADLINES

14 days

Tell POTRAZ if the DPO's contact details change, or if the DPO resigns or is dismissed.²

90 days

Appoint a replacement after a DPO's contract ends.²

Why choose an external DPO?

Certified from day one

Continuity when staff move on

An independent view

An agreed part-time scope

Your organisation always remains responsible for compliance.

Seven Golden Rules

The Act's principles, for everyday decisions, not just paperwork.¹

- 1 Be fair and lawful.** Have a valid reason, such as consent, a contract or a legal duty, before using someone's data.
- 2 Be clear about the purpose.** Use data for the reason you collected it. Don't quietly reuse it for something else.
- 3 Collect only what you need.** Does a routine enquiry really need a copy of someone's ID?
- 4 Keep it accurate.** Correct mistakes promptly when you find them or are told about them.
- 5 Don't keep it forever.** Set retention periods that also respect other record-keeping laws, then dispose of data safely.
- 6 Keep it secure.** Individual logins, access controls, locked cabinets, backups and trained staff.^{1,2}
- 7 Be accountable.** Be able to show how you comply, with records rather than good intentions.



Some Data Needs Extra Care

Start with a lawful basis

Ordinary personal data needs consent, or another ground such as a contract, a legal duty or legitimate interests.¹

● Sensitive data

Health, biometric, genetic and other sensitive data generally need **written consent**, which people can withdraw, subject to legal exceptions.¹

● Children

For under-18s, get consent from a parent or guardian and make reasonable efforts to verify it. Assess the risks regularly, and make no automated decisions that affect a child's rights.²

● Automated decisions

A decision made only by a computer, such as an automatic loan rejection, needs the person's consent or a legal basis.²

● Suppliers

Payroll, hosting and IT providers that handle your data should be bound by a **written agreement** to keep it secure. You stay responsible for what they do.^{1,2}

● Privacy notices

Tell people who is collecting their data, why, and what their rights are, at the point they share it: forms, sign-up pages, reception desks.¹



Respect People's Rights

Everyone whose data you hold has the right to:^{1,2}

Be told	See it	Object
how their information will be used	and get access to the information held about them	to their information being used
Correct it	Delete it	Ask for a human
when the information is wrong	when it is false or misleading	rather than be judged by a computer alone, without consent or a legal basis

Handling a request **well**

- 1 Give people one front door: a named email address or desk.
- 2 Check the person's identity before sharing anything.
- 3 Log every request and your reply in a written procedure.
- 4 Respond promptly. POTRAZ's compliance checklist uses **30 days** as its benchmark.³

When Things Go Wrong

A data breach is any loss, theft, leak or unauthorised access to personal data. It is often ordinary:

A hacked email account

A stolen laptop

A file sent to the wrong person

A lost paper register

Ransomware

THE REPORTING CLOCK

24 hrs

Report to POTRAZ on Form DP3, counted from when you become aware.²

72 hrs

Tell affected people where the breach is likely to pose a high risk to their rights and freedoms.²

14 days

Answer POTRAZ's follow-up requests for more information.²

21 days

Submit your investigation report to POTRAZ.²

In the first hour: escalate, contain the incident safely, preserve evidence and start a record. Don't wait for a full investigation before notifying.

Who in your organisation would report a breach tonight?

Data Leaving Zimbabwe



Using Google Workspace or Microsoft 365, a foreign CRM, HR or accounting system, or reporting to a head office abroad?

Personal data is probably leaving Zimbabwe.

The Act allows transfers only where the receiving country gives adequate protection, or under limited exceptions such as the person's consent or a contract with them.¹ SI 155 requires controllers to notify POTRAZ before transferring or sharing data outside Zimbabwe.²

POTRAZ's guideline **also expects you to:**³

- 1** Notify POTRAZ **before** the transfer, ahead of authorisation.
- 2** Submit a **Data Transfer Impact Assessment**.
- 3** Keep records of every cross-border transfer.
- 4** Host highly sensitive systems, such as **core banking and critical financial systems**, in Zimbabwe unless POTRAZ approves otherwise in writing.

Practical first step: list your cloud and software providers, find out where each stores and accesses your data, and add this to your data map.



What Is At Stake

Up to 7 years

Level 11 fine, up to 7 years' imprisonment, or both, for:²

- Processing without a licence, or failing to renew it
- Giving POTRAZ false information
- Weak security, or an unreported breach
- Breaching SI 155 controller duties, such as notifying transfers or protecting children's data

Up to 2 years

Level 7 fine, up to 2 years' imprisonment, or both, for failing to appoint a DPO.²

Media reports say responsible executives face the prison risk.⁴ A breach also costs customer trust, which is often worth more than any fine.

How POTRAZ inspects³

Routine

At least 7 days' written notice, stating the scope and documents needed.

Unannounced

No prior notice, for example after a complaint, a breach report or suspected unlawful processing.

Voluntary

You invite POTRAZ to assess you, on a date you propose.



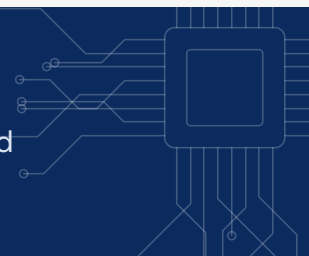
Check Your Readiness

These are the things inspectors typically look for. A “not sure” is a reason to look closer, not proof of a breach.

- ☐ We hold a valid licence in the right tier, with renewal diarised.
- ☐ A certified DPO is appointed and notified to POTRAZ.
- ☐ We have a record of what data we hold, why, where and for how long.
- ☐ People get a clear privacy notice when they share their details.
- ☐ A breach plan names who reports to POTRAZ within 24 hours.
- ☐ Data requests have a written procedure and a log.
- ☐ Suppliers who handle our data have signed data protection agreements.
- ☐ High-risk processing has a data protection impact assessment.
- ☐ Overseas transfers, including cloud services, are notified and assessed.
- ☐ Staff are trained (with records), paper files are locked away, and personal data isn't shared on WhatsApp or email without safeguards.

Fewer than ten ticks?

Ask us for a readiness discussion. We will help you find the gaps and put them in order.



How We Can Help

14 · WORKING WITH US

A scope suited to your organisation, from a one-off readiness review to an ongoing fractional DPO service.

1. Licensing

The right tier, Form DP1 and renewals on time.

2. Fractional DPO

A POTRAZ-certified DPO, notified on Form DP2.

3. Data mapping

What you hold, where, why and for how long.

4. Policies

Privacy notices, consent forms, retention, breach plan.

5. Supplier contracts

Data protection agreements with processors.

6. Risk assessments

DPIAs and cross-border transfer assessments.

7. Staff training

Data protection and cyber awareness, with records.

8. Inspection readiness

Mock audits, gap reports and breach response support.





Sources

1. Cyber and Data Protection Act [Chapter 12:07]. potraz.gov.zw/wp-content/uploads/2026/02/ACT-CDPA.pdf
2. SI 155 of 2024, Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations. potraz.gov.zw/wp-content/uploads/2025/02/si-155-of-2024-Cyber-and-Data-Protection-Normal_240913_1250178.pdf
3. POTRAZ Implementation Guidelines on the Cyber and Data Protection Act (2025): CDPG 1 compliance assessments, CDPG 2 DPO CPD, CDPG 4 cross-border transfers, CDPG 7 MSMEs. veritaszim.net/node/7966
4. POTRAZ Regulatory Notice 2 of 2026 (inspections), as reported by The Herald and Techpoint Africa, 29 July 2026.
5. POTRAZ Regulatory Notice 1 of 2026 (unlicensed processing), as reported by MEA TechWatch, 25 March 2026.

Important disclaimer

This booklet is provided by Berachah Global (“Berachah”) for general awareness and education. It is a simplified overview, not legal advice, a complete statement of the law or a compliance assessment. It was prepared on 13 October 2026 from the sources above, and laws, regulations, guidance, fees and forms may change. Before acting, or deciding not to act, verify the current position against the latest legislation, Government Gazette and POTRAZ publications, and get advice for your circumstances.

Berachah gives no warranty that this summary is complete, accurate or current and, to the fullest extent permitted by law, accepts no liability for loss arising from reliance on it. Nothing excludes liability that cannot lawfully be excluded. This booklet does not create a client, advisory or DPO relationship; services require a separate written agreement, and no regulatory outcome is guaranteed. References to POTRAZ do not imply endorsement or affiliation.



**Speak to us about your
next practical steps.**

EMAIL

info@berachah.global

WEB

www.berachah.global

ZIMBABWE

Unit 4, 25 Shortheath Road, Chisipite,
Harare

+263 777 762 769

Please don't send sensitive client or staff records with a first enquiry.

Client awareness edition · 13 October 2026