Somalia Data Protection Authority

Data Breach Reporting Guidelines

Version: 1.0
Date of Issue: January 2026
Applicability: All Data Controllers and Data Processors
Issued under: Somalia Data Protection Act (Law No. 005 of 2023)

1. Purpose

These Guidelines explain **when, how, and what** organizations must report to the Somalia Data Protection Authority following a personal data breach.

They aim to ensure timely notification, risk-based assessment, and consistent regulatory oversight.

2. What Is a Personal Data Breach?

A personal data breach includes incidents involving:

- Unauthorized access to personal data
- Loss or theft of personal data
- Alteration or corruption of data
- Unlawful disclosure of data
- Accidental or malicious destruction of data

Examples include cyberattacks, human error / accidental emails sent to the wrong person, lost devices, system failures, or insider misuse / unauthorized actions by employees.

3. When Must Organization Report a Breach?

Organizations must notify the DPA **as soon as practicable** and **within 72 hours** of becoming aware of a breach **where the breach poses a risk to individuals**.

Reporting is **mandatory** when the breach:

- Exposes personal data

- Risks the rights, freedoms, or safety of individuals
- Affects the confidentiality, integrity, or availability of personal data

If a breach is not reported within 72 hours, the organization must provide a written justification.

4. When Must Affected Individuals Be Informed?

Organizations must notify affected individuals **without undue delay** if the breach is likely to result in:

- Financial loss or identity theft
- Discrimination
- Reputational harm
- Threats to personal safety
- Misuse of sensitive personal data

Notifications must include clear guidance on how individuals may protect themselves.

5. What Must Be Included in the Breach Report?

Reports submitted to the DPA must include, at a minimum:

- Description of the breach
- Categories and sensitivity of personal data involved
- Estimated number of affected individuals
- Date and method of breach discovery
- Identified risks
- Containment actions taken
- Preventive measures planned
- Status of affected individuals notifications
- Contact details of the DPO or responsible officer

Incomplete reports must be updated as new information becomes available.

6. How to Report a Breach

Organizations can submit breach notifications through:

- Official DPA Breach Notification Form
- Online portal https://dpa.gov.so/breach-report/
- Email: breaches@dpa.gov.so

Supporting documentation (logs, screenshots, evidence, etc.) should be attached where relevant.

7. Record-Keeping Obligations

Organizations must maintain an internal **Breach Register** documenting:

- All breaches, including low-risk incidents
- Assessment outcomes
- Decisions and justifications
- Notifications made
- Remedial actions taken

Records must be retained for **a minimum of five (5) years**.

8. Consequences of Non-Compliance

Failure to report a qualifying breach may result in:

- Administrative fines
- Enforcement notices
- Processing activities restrictions
- Public reprimands
- Other sanctions permitted under the Data Protection Act

9. Support and Assistance

For guidance or clarification:

- Email: breaches@dpa.gov.so
- Official DPA website and portal

Disclaimer

These Guidelines are issued for regulatory guidance and do not limit the statutory powers of the Somalia Data Protection Authority.