MINISTRY OF COMMERCE AND CONSUMER PROTECTION

Legal Metrology Services (LMS)

Data Retention Policy

1. Purpose

This Data Retention Policy establishes the principles, retention periods, and disposal procedures governing the management of data collected, processed, and stored by the Legal Metrology Services (LMS) through its digital system, namely, the Legal Metrology Information System (LMIS). The objective of this Policy is to ensure that data are retained only for as long as necessary to fulfil statutory, operational, legal, evidentiary, audit, and public-interest requirements, while ensuring compliance with applicable laws, data protection obligations, and information security standards.

2. Scope

This Policy applies to all data and records generated, received, or maintained by the LMS in electronic or digitised form, including data processed through online service platforms, internal information systems, databases, and scanned records. It applies to all LMS officers, contractors, service providers, and any third party acting on behalf of LMS.

3. Legal, Regulatory, and Policy Framework

This Policy is guided by, and shall be read in conjunction with, the following (as amended):

- The Legal Metrology Act;
- The Data Protection Act;
- LMS Data Protection / Privacy Policy, which governs the lawful collection, use, disclosure, and storage of personal data;
- The National Archives Act and directives issued by the National Archives Department;
- The Financial Management and Audit framework applicable to public bodies;
- Any other applicable laws, Government policies, and/or Cabinet instructions relating to public sector records management and information security.

4. Principles of Data Retention

LMS shall adhere to the following principles:

- Data shall be collected and retained only for specified, explicit, and lawful purposes in alignment with LMS Data Protection / Privacy Policy;
- Data shall be adequate, relevant, and limited to what is necessary for those purposes;
- Data shall be accurate, and updated as required;
- Data shall not be retained longer than necessary, except where required by law or for legitimate public-interest purposes;
- Data retention and disposal shall follow the Government Security Instructions, standards / measures defined during the LMS implementation and other existing Government procedures to prevent unauthorised access, loss, or corruption.

5. Data Storage and Protection

All records shall be stored securely in digital formats in the Government Online Centre. Sensitive data shall be protected using password controls, restricted access or encryption, as appropriate.

6. Categories of Data and Retention Periods

Specific retention periods are set for each data category, based on statutory, regulatory and business requirements. A retention schedule shall be applicable as detailed hereunder:

Data Category	Retention Period
Service Delivery and Operational Records	10 years from last action or certificate expiry
Enforcement and Compliance Records	10 years after case closure
Financial and Payment Records	10 years
Personal Data of Service Users	Duration of service relationship + 10 years
System, Audit, and Security Logs	7-10 years depending on system criticality
Complaints and Feedback Records	5 years after closure

More details at **Annex**: **Data Retention Schedule Table**

7. Legal Hold

Data subject to a legal hold shall not be destroyed until the hold is lifted. All data under legal hold shall be reviewed every six months and once the litigation concludes, and the hold is lifted, the data shall be released for disposal in accordance with the applicable disposal mechanisms.

8. Rights to access, rectify or request the erasure of subject's data before the expiry of the retention period

An individual may request access to, the rectification of, or the erasure of their data before the expiry of the retention period through the '*Request for Access to or Amendment of Data*' form available on the website of the Legal Metrology Services, subject to the data not being on legal hold, and the request being justified.

9. Archiving

Records with long-term administrative, legal, or historical value shall be archived as per National Archives directives, with access restricted according to Data Protection and Information Security policies.

10. Data Disposal and Destruction

At the end of their retention period, all records shall be securely disposed of through:

a. Secure deletion, anonymisation, or destruction; and
b. Documented disposal processes which shall be auditable and compliant with the Data Protection Act.

No disposal shall be undertaken during ongoing litigation, audit, or statutory hold.

11. Roles and Responsibilities

Designated personnel shall be accountable for managing retention schedules and disposal. All staff shall comply with this Policy – violations or breaches shall be subject to disciplinary action.

Details of each level of responsibility is listed below:

a. **Head of LMS:** Overall accountability for policy compliance;
b. **Data Protection Officer:** Oversight of personal data handling and compliance with Data Protection obligations;
c. **IT Unit / System Administrator:** Implementation of technical controls for retention, archiving, and secure disposal in line with the Government Security Instructions and other existing Government procedures; and
d. **All Officers:** Compliance in daily operations.

12. Access Control and Security

Data retention shall be protected with role-based access, authentication, encryption, and regular security reviews, in line with standards / measures defined during the LMS implementation.

13. Review and Updates

This Policy shall be reviewed every three years or earlier if laws, technology, or operations change. Updates and revisions shall be communicated to all affected employees and teams.

14. Effective Date

This Policy shall take effect as from the date of publication and shall apply to all LMS digital systems, ensuring alignment with LMS Data Protection / Privacy Policy.

Glossary

1. **Data**: Any information collected, generated, or processed by LMS, including personal data, technical data, transactional data, and system logs.
2. **Data Protection Officer**: an officer designated by the Controller under section 22(2)(e) of the Data Protection Act who is responsible for data protection compliance issues.
3. **Disposal**: Secure deletion, anonymisation, or transfer to the National Archives, in accordance with Data Protection and Information Security policies.
4. **Personal Data**: Information relating to an identified or identifiable individual as defined under the Data Protection Act.
5. **Retention Period**: Length of time data must be kept before secure disposal or archival.

09 June 2026

Annex: Data Retention Schedule Table

Data Category	Examples	Retention Period	Policy Alignment
Service Delivery and Operational Records	Applications for, verification, calibration and certificates of suitability, inspection reports, certificates, verification and calibration reports, correspondence	10 years from last action or certificate expiry	Legal Metrology Act, Data Protection Act, LMS Privacy Policy
Enforcement and Compliance Records	Inspection records, notices, seizure/forfeiture records, prosecution documentation	10 years after case closure	Legal Metrology Act, Data Protection Act, LMS Privacy Policy
Financial and Payment Records	Invoices, receipts, online payment records, refunds, accounting data	10 years	Public Finance & Audit framework;
Personal Data of Service Users	Names, identification details, contact information, business particulars of traders, importers, packers, consumers	Duration of service relationship + 10 years	Legal Metrology Act, Data Protection Act, LMS Privacy Policy
System, Audit, and Security Logs	User access logs, system activity records, cybersecurity logs	7-10 years depending on system criticality	Legal Metrology Act, Data Protection Act, LMS Privacy Policy
Complaints and Feedback Records	Consumer complaints, investigation notes, outcomes, correspondence	5 years after closure	Legal Metrology Act, Data Protection Act, LMS Privacy Policy