# Customer Data Retention Policy

# Document Control

## Document Overview

| | |
|---|---|
| Classification: | Public |
| Document Details: | Customer Data Retention Policy |
| Document ID: | EPM035 |
| Author: | Director, Operational Excellence |
| Version: | 4.0 |
| Date of Last Review: | 16th May 2025 |
| Last Reviewed by: | Chief Operating Officer |
| Date of Next Review: | 28th February 2026 |

## Document Approval

The Chief Operating Officer shall review this policy annually and shall determine whether any further changes need to be made prior to approval. Initial release and significant changes require approval from the board.

This Policy was approved by Andy Mackey, Chief Operating Officer on 28th February 2025 and is issued on a version-controlled basis under his signature.

## Document History

| Date of Change | Summary of Change | New Version Number | Changes to be notified to: |
|---|---|---|---|
| 25/02/25 | Annual Review | V3.0 | COO |
| 16/05/25 | Update to reflect recording and transcription of calls | V4.0 | COO |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# 1. Purpose

Effective file-keeping and data management are pivotal to the business functions of EPM Limited. To comply with data protection and privacy legislation, records containing personal data must be:

- Stored appropriately having regard to the sensitivity and confidentiality of the material recorded.
- Retained for only as long as necessary.
- Retrievable and easily traced.
- Disposed of appropriately to ensure that copyrights are not breached and to prevent them falling into the hands of unauthorised personnel.

This policy applies equally to paper, electronic media, call recordings, transcriptions, and any other method used to store personal data.

The period of retention shall only commence when the record is closed or at the request of our customer.

# 2. Storage

All data and records must be securely stored to ensure there is no loss or misuse of the data contained within. All data and records will be stored in the most convenient and appropriate location having the upmost regard for the period of retention required and the frequency with which access will be made to the record.

The degree of security required for file storage will reflect the sensitivity and confidential nature of the data held and recorded. Any data file or record which contains personal data of any form can be considered as confidential in nature. Examples of appropriate storage include password protecting electronic documents and locking paper documents in a secure area.

# 3. Retention

Data and records will not be kept for longer than that which is necessary. The General Data Protection Regulations require that personal data processed for any purpose "shall not be kept for longer than is necessary for that purpose".

Seven years should be regarded as a maximum period of data retention although a shorter period may sometimes be appropriate. No data file or record will be retained for more than seven years after the date of closure unless a valid reason for the extended retention can be demonstrated.

Reasons for extended retention may include:

- If there is a threat of litigation, records likely to be affected should not be amended or disposed of until the threat of litigation has been nullified.
- If records are maintained for the purpose of retrospective comparison e.g., Finance.
- If records contain information relevant to legal action which has started or is yet to reach conclusion.

- If applicable law or statutory body guidance requires an alternative retention period; and
- If records should be archived for historical, industry benchmarking or research purposes.

## 4. Destruction and Disposal

All information of a confidential or sensitive nature must be securely destroyed when no longer required and a register of the disposal of such records maintained. The employee concerned is responsible for doing this. The procedure for the destruction of confidential or sensitive data is as follows:

- Electronic files will be deleted in such a way that they cannot be retrieved by restoring the item from the recycle bin. Destruction of backup copies will also be dealt with.
- Media and equipment should be physically wiped and destroyed prior to disposal.
- Paper will be confidentially stored in confidential wastepaper bins and shredded.

## 5. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, in line with our standard disciplinary procedure, up to and including termination of employment.

## 6. Applicable Policies

This policy is supported by the following policies:

- Data Protection Policy

## 7. Contact Details

Please address any questions or requests relating to this policy to EPM's Data Protection Officer at DPO@epm.co.uk or write to:

Data Protection Officer
EPM Ltd.
Spencer House,
Spitfire Close,
Ermine Business Park,
Huntingdon
PE29 6EP

**End**