Policy on Customer Data Protection

Document Control

Document Overview

Classification:	Public
Document Details:	Policy on Customer Data Protection
Document ID:	EPM037
Author:	Director, Operational Excellence
Version:	3.0
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 25th 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	V2.0	COO
16/05/25	Update to reflect recording and transcription of calls	V3.0	COO

1. Introduction

1.1. EPM will process personal data of customers' employees (which may be held on paper, electronically or otherwise). EPM recognises the need to treat it in an appropriate and lawful manner, in accordance with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). The purpose of this policy is to make you aware of how EPM will handle the personal data of your employees.

1.2. EPM's Data Protection Officer (DPO) is responsible for ensuring compliance with the Data Protection Act 2018 and GDPR and this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to EPM's DPO

2. Definitions

2.1. Data is information which is stored electronically, in paper-based filing systems, in audio recordings (such as telephone call recordings), or in derived formats such as transcriptions.

2.2. Data subjects for the purpose of this policy include all living individuals about whom EPM holds personal data. All data subjects have legal rights in relation to their personal information.

2.3. Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in EPM's possession). Personal data can be factual (for example, a name and address or date of birth) or it can be an opinion about that person, their actions and behaviour.

2.4. Data controllers are the people who determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies relating to the Data Protection Act 2018 and the General Data Protection Regulation.

2.5. Data users are EPM employees whose work involves processing personal data. EPM data users are obliged to comply with this policy when processing customers' personal data. Any breach of this policy by an EPM data user may result in disciplinary action.

2.6. Data processors include any person or organisation that is not a data user that processes customers' personal data on EPM's behalf and on EPM's instructions e.g. DfE, TPA.

2.7. Processing is any activity that involves the use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring data to third parties.

2.8. Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or

proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions.

3. Data Protection Principles

3.1. Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

a) Processed fairly and lawfully

b) Proceed for limited purposes and in an appropriate way

c) Adequate, relevant and not excessive for the purpose

d) Accurate

e) Not kept longer than necessary for the purpose

f) Secure

g) Not transferred to people or organisations situated in countries without adequate protection

4. Obtaining Information

4.1. EPM will process data about customers' employees in accordance with the contract for services and to assist customers in meeting their legal obligations as an employer, e.g. to provide contractual and other employment documentation, and pay employees.

4.2. We may process sensitive personal data relating to customer employees including, as appropriate:

a) Information about an employee's physical or mental health or condition in order to monitor sick leave and provide customers with the information to make decisions as to the employee's fitness for work.

b) The employee's racial or ethnic origin or religious or similar information in order to assist the customer with monitoring compliance with equal opportunities legislation.

c) In order to comply with legal requirements and obligations to third parties.

5. Purposes of Information and Length of Time Retained

5.1. Personal data of customer employees will be processed in accordance with the Data Protection Principles and will be processed with the consent of the individual, such consent will be obtained by the customer. The customer will have in place a policy for personal information/data protection for their employees (for example EPM Model Policy on Personal Information). EPM will not keep personal data of customer employees longer than necessary for the purpose or purposes for which they were collected, but may retain personal data of customer employees for 7 years from

termination (or longer where there is a legal risk or requirement, or a statutory or safeguarding requirement).

5.2. EPM will take all reasonable steps to destroy or erase from our systems, all data which is no longer required in accordance with our Customer Data Retention Policy.

5.3. EPM is registered with the Information Commissioner's Office for all the purposes for which it processes personal data.

6. Nature of Information

6.1. EPM will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

6.2. EPM expects customers to ensure that Personal Data held about their employees is accurate, up to date and checked at regular intervals. EPM will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data in accordance with our Customer Data Retention Policy.

7. Disclosure of Information

7.1. Personal data will be used only for the purpose for which it was gathered, unless the consent of the people concerned has been obtained to a new or varied use.

7.2. Routine disclosures will be specified on the Data Protection register and in the customer's own Data Protection publication scheme and consent will be deemed to have been given to routine disclosures so included.

7.3. In other cases the explicit consent of the data subject will be obtained in writing. Confirmation of consent by telephone is acceptable if a written request has been received which implies the consent of the data subject.

7.4. Access to personal data is restricted to those who, in the view of EPM, have a legitimate need to access it and a request will be refused if the data user is uncertain whether the person requesting access, including another member of the customer's employees, is entitled to it.

8. Access to Personal Files

8.1. Should a customer staff member make a formal written application to EPM about their Personal Data, the DPO will handle such request in accordance with the provisions of the Data Protection Act 2018 and the General Data Protection Regulation. The identity of the person requesting the Personal Data shall be established.

8.2. Information which would disclose the identity of a third person is exempt from access, unless the consent of the source is available or it is reasonable in all the circumstances to comply with the subject access request without the third party's consent under Schedule 2of the DPA 2018. Personal data may be exempt for other

reasons under the Data Protection Act 2018 and these are detailed in Schedules 2-4.

8.3. Requests for access to personal data will be dealt with within one month of receipt of sufficient information to process the request

9. Standards of Security

9.1. EPM will determine and maintain an appropriate level of security for its premises, equipment, network, programs, data and documentation, and will ensure that access to them is restricted to appropriate employees.

10. Training and Policies

10.1. All new and existing employees who handle personal data will receive training on data protection procedures, which includes information about the standards EPM expects its employees to observe in the use of personal data.

11. DBS Processing

11.1. EPM complies with the Disclosure and Barring Service (DBS) Code of Practice (as amended). In accordance with section 124 of the Police Act 1997, certificate information is only discussed with those who are authorised to discuss it in the course of their duties. We maintain a record of all customer DBS Liaison Officers and others with authority to discuss DBS Certificate Information. EPM employees are aware that that it is a criminal offence to share DBS Certificate Information with anyone who is not entitled to access.

12. Review of Policy

12.1. This policy shall be reviewed as necessary. EPM reserves the right to change this policy at any time.

End