EPM Data Protection Policy

EPM Data Protection Policy

Review History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Amendments/Comments | Reviewer/s |
| January 2018 | 1.0 | Initial Draft | M Eastwood |
| May 2018 | 2.0 | Final Version | R O’Driscoll |
|  |  |  |  |
|  |  |  |  |

Contents

[1. Introduction 4](#_Toc131168786)

[2. Applicability 4](#_Toc131168787)

[3. Policy Scope 4](#_Toc131168788)

[4. Responsibilities 4](#_Toc131168789)

[5. Definitions 5](#_Toc131168790)

[6. Obtaining Information 6](#_Toc131168791)

[7. Process Sensitive Personal Data Relating to Employees 6](#_Toc131168792)

[8. Principles Relating to Processing of Personal Data 7](#_Toc131168793)

[9. Purposes of Information and Length of Time Retained 7](#_Toc131168794)

[10. Nature of Information 7](#_Toc131168795)

[11. Disclosure of Information 7](#_Toc131168796)

[12. Data Breach 8](#_Toc131168797)

[13. Individual Rights 8](#_Toc131168798)

[14. Access to Personal Files 9](#_Toc131168799)

[15. Data Security and Impact Assessment 9](#_Toc131168800)

[16. Monitoring Activities 10](#_Toc131168801)

[17. Request for Data by Public Authorities 10](#_Toc131168802)

[18. Training 10](#_Toc131168803)

[19. Review of Policy 11](#_Toc131168804)

[20. Other Related Documents: 11](#_Toc131168805)

[21. Relevant Contacts 11](#_Toc131168806)

1. Introduction

This policy details the roles and responsibilities of all employees, workers and contractors acting on behalf of EPM Ltd (“Organisation”), regarding the protection of personal data. EPM is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

1. Applicability

This policy applies to all EPM employees at all levels and grades, including directors, employees, contractors, trainees, seconders, home-workers, part-time and fixed-term employees, and agency staff (collectively known as “Staff” or “Employee” in this policy and any associated policies), and third parties such as IT support companies who have access to EPM’s systems and information under the contract. Information can be in many forms including electronic documents, printed/handwritten documents and spoken information. Information contained in any form has value to the Company and therefore is protected under this policy. Failure to adhere to the Data Protection Policy is considered a serious breach of Company policy, and may result in disciplinary action, including dismissal.

1. Policy Scope

To meet the requirements of the GDPR and other related data protection legislation, this policy applies to electronic and paper records held in structured filing systems containing personal data, meaning data which relates to living individuals who can be identified from the data. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings and to any electronic/online identifiers that can be used to identify an individual.

1. Responsibilities

EPM must:

* Manage and process personal data properly.
* Protect the individual's rights to privacy.
* Provide an individual with access to all personal information held on them.

EPM has a legal responsibility to comply with the law, including the Data Protection Act 2018 and the General Data Protection Regulation. The individual with overall responsibility for this policy is the Data Protection Officer. EPM is named as the Data Controller under the Act however much of the work undertaken by EPM may be as an appointed Data Processor.

EPM is required to notify the Information Commissioner of the processing of personal data; this is included in a public register. The public register of data controllers is available on the Information Commissioner's website.

EPM’s Data Protection Officer is responsible for drawing up guidance on good data protection practice and promoting compliance with this guidance through advising employees on the creation, maintenance, storage, and retention of their records which contain personal information.

Every employee that holds, or has access to, information about identifiable living individuals must comply with data protection legislation in managing that information. Individuals can be liable for breaches of the Act. All EPM employees are responsible to act in accordance with EPM’s policies, procedures, and guidelines and within the provisions of the Data Protection Act 2018 and the General Data Protection Regulation.

1. Definitions

In this policy, unless otherwise stated or unless the context otherwise requires, each term will have the meaning set out below:

Data protection means practices and operations relating to the fair and lawful treatment of personal data and an understanding of the regulatory requirements relating to data privacy.

Personal data is data which relates to a living individual who can be identified:

* from this data; or
* from this data and other information, which is in the possession of, or is likely to come into the possession of the data controller.

Examples of personal data can include, but are not limited to:

* names
* addresses
* telephone numbers
* dates of birth
* National Insurance numbers
* employee numbers
* named email addresses.
* account details
* CCTV images
* photographs
* personal opinions
* internet browsing history
* static/dynamic IP addresses

Special Categories of personal data (also known as sensitive personal data) includes:

* racial or ethnic origin
* political opinions
* religious or philosophical beliefs
* trade union membership
* the processing of genetic data
* biometric data for uniquely identifying an individua
* data concerning health or data concerning an individual’s sex life
* sexual orientation
* medical information.

Additionally, although not sensitive under data protection legislation, financial data and information relating to criminal convictions should also be treated with additional safeguards. due to their associated risks.

Data processing in relation to information or data, means obtaining, recording or holding the information/data or carrying out any operation or set of operations on the information/data, including:

* organisation, adaptation, or alteration of the information/data.
* retrieval, consultation, or use of the information/data.
* disclosure of the information or data by transmission, dissemination or otherwise making
* available.
* alignment, combination, blocking, erasure or destruction of the information or data; or
* storage of information or data, whether electronically or manually (paper based).

**Data subject** an individual who is the subject of personal data.

**Data controller** means a person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which and the way any personal data is, or is to be, processed.

**Data processor** in relation to personal data, means any person or organisation (other than an employee of the data controller) who processes the data on behalf of the data controller.

**Relevant filing system** means any paper-based records which are structured in a way which is either:

* By reference to the individual by name or code.
* By reference to criteria relating to individuals
1. Obtaining Information

The organisation will process data about employees for legal, administrative and management. purposes and to enable us to meet our legal obligations as an employer, for example to pay, monitor performance and to confer benefits in connection with employment.

1. Process Sensitive Personal Data Relating to Employees

The organisation may process sensitive personal data relating to employees including, as appropriate:

1. information about an employee's physical or mental health or condition to monitor sickness absence and take decisions as to the employee's fitness for work.
2. the employee's racial or ethnic origin or religious or similar information to monitor compliance with equal opportunities legislation.
3. to comply with legal requirements and obligations to third parties.
4. Principles Relating to Processing of Personal Data

In line with GDPR, anyone processing personal data must comply with the following principles. It is our policy that personal data must be:

1. processed lawfully, fairly and in a transparent manner (‘lawfulness, fairness and transparency’)
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed (‘data minimisation’).
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is
5. processed, is erased, or rectified without delay (‘accuracy’); kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

The Board of Directors shall be responsible for and must be able to demonstrate compliance. with, these principles.

1. Purposes of Information and Length of Time Retained

Personal data will be held in accordance with EPM’s Policy on Retention of Personal Information. We will not keep personal data longer than necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy or erase from us. systems, all data which is no longer required.

The Board of Directors will state the purposes for which it holds personal information and will. register with the Data Protection Commissioner all the purposes for which it processes personal data.

1. Nature of Information

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

We 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 the EPM Data Retention Policy.

1. Disclosure of Information

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

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

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.

Access to personal data will be refused if the data user is uncertain whether the person requesting access, including another employee, is entitled to it. In such a case, the request must be referred to the Data Officer for consideration before the request is rejected.

1. Data Breach

If we discover that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, the Data Protection Officer will report it to the Information.

Commissioner within 72 hours of discovery.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, all affected individuals will be informed of the breach and provided with information including the type of data and likely consequences of the breach, plus mitigating steps taken.

Any breach of the policy will be fully investigated, and remedial steps taken to ensure a similar breach cannot happen again.

A record of all data breaches, regardless of their size or effect, will be retained within the Breach. Register.

1. Individual Rights

As a data subject, individuals have several rights in relation to their personal data.

* 1. Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell them:

* whether or not their data is processed and if so why, the categories of personal.
* data concerned and the source of the data if it is not collected from the individual.
* to whom their data is or may be disclosed, including to recipients located outside.
* the European Economic Area (EEA) and the safeguards that apply to such transfers.
* for how long their personal data is stored (or how that period is decided); their rights to rectification or erasure of data, or to restrict or object to processing.
* their right to complain to the Information Commissioner if they think the
* organisation has failed to comply with their data protection rights; and
* whether or not the organisation carries out automated decision-making and the
* logic involved in any such decision-making.

The organisation will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically unless they agree otherwise.

If the individual requests additional copies, the organisation reserves the right to charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.

To make a subject access request, the individual should send the request to dpo@epm.co.uk . In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify their identity and the documents it requires.

The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the organisation processes large amounts of the individual's data, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify them that this is the case and whether it will respond to it.

* 1. Other rights

Individuals have several other rights in relation to their personal data. They can require the organisation to:

* rectify inaccurate data.
* stop processing or erase data that is no longer necessary for the purposes of processing.
* stops processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data).
* stop processing or erase data if processing is unlawful; and
* stop processing data for a period if data is inaccurate or if there is a dispute about whether the individual's interests override the organisation's legitimate grounds for processing data.

To ask the organisation to take any of these steps, the individual should send the request to DPO@epm.co.uk

1. Access to Personal Files

Employees are entitled to know if the organisation holds information about them. Any request for information must be made formally in writing addressed to EPM’s Data Protection Officer, the Data Subject Access Request (DSAR) Procedure sets out further information regarding this.

1. Data Security and Impact Assessment

The organisation will determine and maintain an appropriate level of security (and back–up) for its premises, equipment, network, programs, data and documentation, and will ensure that access to them is restricted to appropriate individuals. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

1. Monitoring Activities

The organisation will record and monitor usage of all company IT equipment, user activity, voice traffic, email, and internet usage as deemed necessary.

Those responsible for undertaking the monitoring will observe the strictest confidentiality when undertaking these activities. The report will be made directly to DPO@epm.co.uk , who will determine any action that may need to be taken.

Monitoring of IT equipment, electronic data, telephone calls, emails, internet access, network access and remote access will be carried out to ensure that usage is in accordance with EPM’s policies, procedures, and guidelines.

1. Request for Data by Public Authorities

Requests for personal data may come from public authorities, including but not limited to the following:

* the Police.
* the Department of Work and Pensions.
* the UK Border Agency.
* HM Revenue & Customs.
* Local Authorities.
* DVLA.

Requests received from a public authority will only be processed when submitted in writing, including electronic communication. Such requests for data usually require that the organisation does not inform, or gather consent from, the data subject when responding to the request. When a request is received, this should first be referred to the Data Protection Officer who will ensure that the request is valid.

Data can only be disclosed without the knowledge and consent of the data subject where it is processed for either the:

* prevention or detection of crime.
* apprehension or prosecution of offenders; or
* assessment or collection of tax or duty.

Additionally, it must be shown that informing or gathering consent from the data subject would likely prejudice the crime or taxation purposes.

Where these conditions are not met, the Data Protection Officer may decide to not disclose the data. Where the Data Protection Officer decides the records should not be disclosed or only partially disclosed, they must record in writing their reasons. A public authority may have a Court Order issued for the disclosure of documents. Any objections should be recorded along. With the Court Order however the data should be disclosed.

1. Training

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

1. Review of Policy

This policy shall be reviewed as necessary. We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by email.

1. Other Related Documents:

This policy is supported by the following documents:

* Data Subject Access Request (DSAR) Procedure
* Relevant Data Privacy Notices
* Code of Conduct
1. Relevant Contacts:

Data Protection Officer

Please refer any queries, issues or requests received to the EPM Data Protection Officer:

Data Protection Officer

EPM Ltd.

St John’s House,

Spitfire Close,

Ermine Business Park,

Huntingdon,

Cambridgeshire

PE29 6EP

ICO Contact Details

If you require more information about the General Data Protection Regulation, the Data Protection Act 2018, or are unhappy with the way EPM has dealt with your data please contact:

The Information Commissioner

Wycliffe House,

Water Lane,

Wilmslow,

Cheshire

SK9 5AF

[www.ico.org.uk](http://www.ico.org.uk)