GDPR POLICY & PROCEDURE MANUAL

EPM ESTATES
Unit 3 JFK House,
John F Kennedy Road,
Bluebell,
Dublin 12. D12 C966

01 440 8652
www.EPM Estates.ie

Effective Date:	Next Revision Date:	Signature:
15/10/2020	15/10/2022	

Policies Included:

DATA SUBJECT ACCESS REQUEST POLICY AND PROCEDURE

CONTENTS

1 PURPOSE

1.1 This policy and procedure establishes an effective, accountable and transparent framework for ensuring compliance with the requirements for the data subject access request policy by the *GDPR*.

2 SCOPE

2.1 This policy and procedure applies across all entities or subsidiaries owned, controlled, or operated by company and to all employees, including part-time, temporary, or contract employees, that handle personal data.

3 POLICY STATEMENT

3.1 The GDPR details rights of access to both manual data (which is recorded in a relevant filing system) and electronic data for the data subject. This is known as a Data Subject Access Request (DSAR).

3.2 Under the GDPR, organisations are required to respond to subject access requests within one month. Failure to do so is a breach of the GDPR and could lead to a complaint being made to the Data Protection Regulator.

3.3 This policy informs staff of the process for supplying individuals with the right of access to personal data and the right of access to staff information under the General Data Protection Regulation (hereinafter called GDPR). Specifically:

- All staff need to be aware of their responsibilities to provide information when a data subject access request is received. When a subject access request is received, it should immediately be reported to the Data Protection Manager to log and track each request.
- Requests must be made in writing (template form is provided, but not mandatory).
- The statutory response time is one month.
- Requests should include the full name, date of birth and address of the person seeking access to their information. To comply with the GDPR, information relating to the individual must only be disclosed to them or someone with their written consent to receive it.
- No fee can be charged for initial DSAR for all types of records, whether manual or electronic format.

4 PROCEDURE

How should DSARs be processed after receiving

When a subject access request is received from a data subject it should immediately be reported to the Data Protection Manager who will log and track each request. If you are asked to provide information, you will need to consider the following before deciding how to respond:

- Under GDPR Articles 7(3), 12, 13, 15-22 data subjects have the following rights:
  - to be informed;
  - to access their own data;
  - to rectification;
  - to erasure (Right to be Forgotten);
  - to restriction of processing;
  - to be notified;
  - to data portability;

- to object;
- to object to automated decision making.

- Requests must be made in writing (template form is attached but is not mandatory). All DSARs received by email, mail, fax, social media, etc. must be processed.
- The type of access you must provide may vary depending on how the records held. It does not have to state 'subject access request' or 'data protection' to constitute a request under the GDPR.
- If a request has already been complied with and an identical or similar request is received from the same individual a fee can be charged for the second request unless a reasonable interval has elapsed.
- The statutory response time is one month.
- Requests should include the full name, date of birth and address of the person seeking access to their information. To comply with the GDPR, information relating to the individual must only be disclosed to them or someone with their written consent to receive it.
- Before processing a request, the requestor's identity must be verified. Examples of suitable documentation include:
  - Valid Passport
  - Valid Identity Card
  - Valid Driving Licence
  - Birth Certificate along with some other proof of address, e.g. a named utility bill (no longer than 3 months old)

Fees

4.1 No fee can be charged for providing information in response to a data subject access request, unless the request is 'manifestly unfounded or excessive', in particular, because it is repetitive. If the company receives a request that is manifestly unfounded or excessive, it will charge a reasonable fee taking into account the administrative costs of responding to the request. Alternatively, the company will be able to refuse to act on the request.

Subject access requests made by a representative or third party

4.2 Anyone with full mental capacity can authorise a representative/third party to help them make a data subject access request. Before disclosing any information, the company must be satisfied that the third party has the authority to make the request on behalf of the requestor and that the appropriate authorisation to act on their behalf is included (see *Data Request Form*).

Complaints

4.3 If an individual is dissatisfied with the way the company have dealt with their subject access request, they should be advised to invoke the company complaints process. If they are still dissatisfied, they can complain to the Data Protection Regulator.

5 RESPONSIBILITIES

Compliance, monitoring and review

5.1 The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing subject access rights at the company rests with the Data Protection Manager.

5.2 All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant company policies and procedures.

Records management

5.3 Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised recordkeeping system.

5.4 All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

6 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Manager (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

DSAR: data subject access request

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

7 RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

8 FEEDBACK AND SUGGESTIONS

8.1 Company employees may provide feedback and suggestions about this document by emailing Thomas Horan <thoran@ EPM Estates.ie>.

9 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Thomas Horan
Data Protection Manager	Thomas Horan
Next Review Date	15/10/2020

DATA BREACH NOTIFICATION POLICY AND PROCEDURE

CONTENTS

10 PURPOSE

This policy and procedure establishes an effective, accountable and transparent framework for ensuring compliance with the requirements for data breach notification policy by the *GDPR.*

11 SCOPE

This policy and procedure applies across all entities or subsidiaries owned, controlled, or operated by the company and to all employees, including part-time, temporary, or contract employees, that handle data breach notifications.

12 POLICY STATEMENT

Any staff member who suspects that a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data might have occurred, must immediately notify the Data Protection Manager and provide a description of the circumstances. Notification of the incident can be made via e-mail, by telephone, or in person.

The Data Protection Manager will investigate all reported incidents to confirm whether a personal data breach has occurred. If a personal data breach is confirmed, the Data Protection Manager will follow the data breach notification procedure based on the criticality and quantity of the personal data involved. For severe personal data breaches, the Executive Team will initiate and chair an emergency response team to coordinate and manage the personal data breach response.

13 NOTIFICATION PROCEDURE

13.1 All personal data breaches must be reported immediately to the Data Protection Manager.

13.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Manager must ensure that the Data Protection Regulator is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

13.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Art 3.2) to the rights and freedoms of data subjects, the Data Protection Manager must ensure that all affected data subjects are informed of the breach directly and without undue delay.

13.4 Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The contact details of the company's Data Protection Manager;
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by the company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

14 RESPONSIBILITIES

Compliance, monitoring and review

14.1 The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing data transfer activities rests with the Data Protection Manager.

14.2 All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant company policies and procedures.

Records management

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised company recordkeeping system.

All records relevant to administering this policy and procedure will be maintained for a period of 5 years unless stated otherwise.

15 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Manager: an / or has access to an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

16 RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- The company Data Protection Policy

17 FEEDBACK AND SUGGESTIONS

17.1 The company employees may provide feedback and suggestions about this document by emailing: Thomas Horan <thoran@EPM Estates.ie>

18 APPROVAL AND REVIEW DETAILS

Approval and Review	**Details**
Approval Authority	Thomas Horan
Data Protection Manager	Thomas Horan
Next Review Date	15/10/2022

DATA PROTECTION IMPACT ASSESSMENT POLICY AND PROCEDURE

CONTENTS

19 PURPOSE

This policy and procedure establishes an effective, accountable and transparent framework for ensuring compliance with the requirements for data protection impact assessment by the GDPR.

20 SCOPE

This policy and procedure applies across all entities or subsidiaries owned, controlled, or operated by the company and to all employees, including part-time, temporary, or contract employees, that handle personal data.

21 POLICY STATEMENT

Data Protection Impact Assessments (DPIA) are used to identify and mitigate against any data protection related risks arising from a new project, service, product, or process, which may affect the organization (Data Controller) or the individuals (Data Subjects).

When is DPIA necessary

21.1 DPIA is necessary:

- Before the implementation of new technologies or processes, or before the modification of existing technologies or processes;
- Data processing is likely to result in a high risk to the rights and freedoms of individuals.

21.2 Processing that is likely to result in a high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals;
- Large scale processing of special categories of data or personal data relating to criminal convictions or offences;
- Large scale, systematic monitoring of public areas (CCTV).

Should the Regulator be consulted on completion of the DPIA?

21.3 If during the DPIA process, the Data Controller has identified and taken measures to mitigate any risks to personal data, it is not necessary to consult with the Regulator before proceeding with the changes.

21.4 If the DPIA suggests that any identified risks cannot be managed and the residual risk remains high, you must consult with the Regulator before moving forward with the project.

21.5 Regardless of whether consultation with the Regulator is required, your obligations of retaining a record of the DPIA and updating the DPIA in due course remain.

21.6 Even if consultation is not required, the DPIA may be reviewed by the Regulator at a later date in the event of an audit or investigation arising from your use of personal data.

22 PROCEDURE

Steps for conducting DPIA

22.1 **Describe data flows.** Identify how personal information will be collected, stored, used and deleted as part of the new (or modified) system or process. Identify what kinds of data will be

used as part of the new (or modified) system or process and who will have access to the data. *Populate Section 1 of the Data Protection Impact Assessment (DPIA) Form.*

22.2 **Identify data protection and related risks.** Identify all risks to Data Subjects or to the organization (Data Controller) that are related to personal data protection. For each risk assign a risk category (High/Medium/Low) and *populate the appropriate columns in Section 2 of the Data Protection Impact Assessment (DPIA) Form.*

22.3 **Assign risk mitigation measures.** For each risk assign risk mitigation measures. Focus on mitigating measures for risks with High and Medium impact category. *Populate the last column in Section 2 of the Data Protection Impact Assessment (DPIA) Form.*

22.4 **Further actions.** Consider if the Regulator should be consulted for the DPIA. Plan regular DPIA reviews and updates.

23 RESPONSIBILITIES

Compliance, monitoring and review

23.1 The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing data protection impact assessment activities for the company rests with the Data Protection Manager.

23.2 All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant company policies and procedures.

Records management

23.3 Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised company recordkeeping system.

23.4 All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

24 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Manager (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

25 RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

26 FEEDBACK AND SUGGESTIONS

26.1 Company employees may provide feedback and suggestions about this document by emailing Thomas Horan <thoran@EPM Estates.ie>.

27 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Thomas Horan
Data Protection Manager	Thomas Horan
Next Review Date	15/10/2022

Data Processing Agreement

This Agreement (the "Agreement") is made and entered into this date: ("Effective Date") by and between EPM Estates with its principal place of business located at Unit 3 JFK House, John F Kennedy Road, Bluebell, Dublin 12. D12 C966 (the Controller – hereinafter referred to as the "Client") and [insert name] with its principal place of business located at [insert address] (the Processor - hereinafter referred to as the "Supplier") (hereinafter referred to individually as a "Party" and collectively as "the Parties").

Please Note

The specific provisions according to Article 28 Paragraph 3 GDPR should be incorporated into the Agreement in their entirety and be used as a Checklist. The alternatives applicable for the specific service relationship should be ticked. Empty fields are to be filled in as applicable to the specific requirements of each individual Order or Contract. Systems of payment and liability conditions concerning the specific services of the Supplier should be agreed in the main contract.

1. Subject matter and duration of the Order or Contract

(1) Subject matter

☐ The Subject matter of the Order or Contract results from the Service Agreement …….. dated ……., which is referred to here (hereinafter referred to as Service Agreement).

or

☐ The Subject matter of the Order or Contract regarding the processing of data is the execution of the following services or tasks by the Supplier …… *(Definition of the services or tasks)*

(2) Duration

☐ The duration of this Order or Contract corresponds to the duration of the Service Agreement.

or *(specifically, if no Service Agreement regarding the Duration exists)*

☐ The Order or Contract will be authorised for one-time execution only.

or

☐ The Duration of this Contract is limited to …….. .

or

□ The Contract is authorised for an unlimited period and can be cancelled by either Party with a notice period of…… (time period) to ……. (deadline) . This does not prejudice the right to termination of the contract without notice.

2. Specification of the Order or Contract Details

(1) Nature and Purpose of the intended Processing of Data

☐ Nature and Purpose of Processing of personal data by the Supplier for the Client are precisely defined in the Service Agreement dated ……..

or

☐ Detailed description of the Subject Matter with regard to the Nature and Purpose of the services provided by the Supplier: .....

The undertaking of the contractually agreed Processing of Data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled. The adequate level of protection in .....*(e.g. country, territory or specific sectors within a country)*

☐ has been decided by the European Commission (Article 45 Paragraph 3 GDPR);

☐ is the result of binding corporate rules (Article 46 Paragraph 2 Point b in conjunction with Article 47 GDPR);

☐ is the result of Standard Data Protection Clauses (Article 46 Paragraph 2 Points c and d GDPR);

☐ is the result of approved Codes of Conduct (Article 46 Paragraph 2 Point e in conjunction with Article 40 GDPR);

☐ is the result of an approved Certification Mechanism. (Article 46 Paragraph 2 Point f in conjunction with Article 42 GDPR).

☐ is established by other means ..... (Article 46 Paragraph 2 Point a, Paragraph 3 Points a and b GDPR)

(2) Type of Data

☐ The type of personal data used is precisely defined in the Service Agreement under: …..

or

☐ The Subject Matter of the processing of personal data comprises the following data types/categories (List/Description of the Data Categories)

- □ Personal Master Data (Key Personal Data)
- □ Contact Data
- □ Key Contract Data (Contractual/Legal Relationships, Contractual or Product Interest)
- □ Customer History
- □ Contract Billing and Payments Data
- □ Disclosed Information (from third parties, e.g. Credit Reference Agencies or from Public Directories...
- □ Other: … (Please specify)

(3) Categories of Data Subjects

☐ The Categories of Data Subjects are precisely defined in the Service Agreement under: .....

or

☐ The Categories of Data Subjects comprise:

- □ Customers
- □ Potential Customers
- □ Subscribers
- □ Employees
- □ Suppliers
- □ Authorised Agents
- □ Contact Persons
- □ Other: ... (Please specify)

3. Technical and Organisational Measures

(1) Before the commencement of processing, the Supplier shall document the execution of the necessary Technical and Organisational Measures, set out in advance of the awarding of the Order or Contract, specifically with regard to the detailed execution of the contract, and shall present these documented measures to the Client for inspection. Upon acceptance by the Client, the documented measures become the foundation of the contract. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

(2) The Supplier shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account. (Details in Appendix 1)

(3) The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative

adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

4. Rectification, restriction and erasure of data

(1) The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Client, but only on documented instructions from the Client.
Insofar as a Data Subject contacts the Supplier directly concerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the Data Subject's request to the Client.

(2) Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Client without undue delay.

5. Quality assurance and other duties of the Supplier

In addition to complying with the rules set out in this Order or Contract, the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

a) Appointed Data Protection Manager, who performs his/her duties in compliance with Articles 38 and 39 GDPR.
   - ☐ The Client shall be informed of his/her contact details for the purpose of direct contact. The Client shall be informed immediately of any change of Data Protection Manager.
   - ☐ The Supplier has appointed Thomas Horan <thoran@EPM Estates.ie> as Data Protection Manager. The Client shall be informed immediately of any change of Data Protection Manager.
   - ☐ His/Her current contact details are always available and easily accessible on the website of the Supplier.

b) The Supplier is not obliged to appoint a Data Protection Manager but will provide designated Contact Person on behalf of the Supplier.

c) If the Supplier is established outside the EU & EEA the client will designate a Representative within the Union pursuant to Article 27 Paragraph 1 GDPR: And provide the details to the Client.

d) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Supplier entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Client, which includes the powers granted in this contract, unless required to do so by law.

e) Implementation of and compliance with all Technical and Organisational Measures necessary for this Order or Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR [details in Appendix 1].

f) The Client and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.

g) The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Order or Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative

Rule or Regulation regarding the processing of personal data in connection with the processing of this Order or Contract.

h) Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract data processing by the Supplier, the Supplier shall make every effort to support the Client.

i) The Supplier shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

j) Verifiability of the Technical and Organisational Measures conducted by the Client as part of the Client's supervisory powers referred to in item 7 of this contract.

6. Subcontracting

(1) Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Supplier shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

(2) The Supplier may commission subcontractors (additional contract processors) only after prior explicit written or documented consent from the Client.

a) Subcontracting is not permitted.

b) The Client agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

Company subcontractor	Address/ Country	Service

c) Outsourcing to subcontractors or

Changing the existing subcontractor
are permissible when:

- The Supplier submits such an outsourcing to a subcontractor to the Client in writing or in text form with appropriate advance notice; and
- The Client has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to the Supplier; and
- The subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

(3) The transfer of personal data from the Client to the subcontractor and the subcontractor's commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.
(5) Further outsourcing by the subcontractor

- ☐ Is not permitted;
- ☐ Requires the express consent of the main Client (at the minimum in text form);
- ☐ Requires the express consent of the Supplier (at the minimum in text form);

All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

7. Supervisory powers of the Client

(1) The Client has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.
(2) The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR**.** The Supplier undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.
(3) Evidence of such measures, which concern not only the specific Order or Contract, may be provided by

- ☐ Compliance with approved Codes of Conduct pursuant to Article 40 GDPR;
- ☐ Certification according to an approved certification procedure in accordance with Article 42 GDPR;
- ☐ Current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Manager, IT security department, data privacy auditor, quality auditor)
- ☐ A suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI)) or ISO/IEC 27001).

(4) The Supplier may claim remuneration for enabling Client inspections.

8. Communication in the case of infringements by the Supplier

(1) The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.

b) The obligation to report a personal data breach immediately to the Client

c) The duty to assist the Client with regard to the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.

d) Supporting the Client with its data protection impact assessment

e) Supporting the Client with regard to prior consultation of the supervisory authority

(2) The Supplier may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of the Supplier.

9. Authority of the Client to issue instructions

(1) The Client shall immediately confirm oral instructions (at the minimum in text form).
(2) The Supplier shall inform the Client immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

10. Deletion and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Service Agreement, the Supplier shall hand over to the Client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.
(3) Documentation which is used to demonstrate orderly data processing in accordance with the Order or Contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Client at the end of the contract duration to relieve the Supplier of this contractual obligation.

28 Appendix - Technical and Organisational Measures

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

- **Physical Access Control**
  No unauthorised access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems
- **Electronic Access Control**
  No unauthorised use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media
- **Internal Access Control** (permissions for user rights of access to and amendment of data)
  No unauthorised Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorisation concept, need-based rights of access, logging of system access events
- **Isolation Control**
  The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Client support, sandboxing;
- **Pseudonymisation** (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)
  The processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

- **Data Transfer Control**
  No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;
- **Data Entry Control**
  Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

- **Availability Control**
  Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning
- **Rapid Recovery** (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR);

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

- **Data Protection Management;**
- **Incident Response Management;**
- **Data Protection by Design and Default** (Article 25 Paragraph 2 GDPR);
- **Order or Contract Control**
  No third-party data processing as per Article 28 GDPR without corresponding instructions from the Client, e.g.: clear and unambiguous contractual arrangements,

formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.

Signed for and on behalf of: EPM Estates	Signed for and on behalf of: [insert name of Supplier]
_____	_____
Name: Title: Date:	Name: Title: Date:

Data Protection Manager

JOB DESCRIPTION

Job title	Data Protection Manager or Data Protection Manager (DPO)
Department	Compliance
Reporting to	THOMAS HORAN
Professional Assistance	Acceptable provided Data Protection Manager is involved.
Job summary	To provide direction, support and advice to EPM Estates Principal Officers, Heads of Service and all departments across the company in relation to their data protection obligations. To take the lead role in the management and implementation of data protection compliance as well as overseeing compliance with the General Data Protection Regulations (GDPR). To act as the project manager for the implementation of the General Data Protection Regulations. The Data Protection Manager post will not be a protected role. The Company shall do its best to ensure that the position does not receive any instructions that will prevent the Data Protection Manager from performing the exercise of the main tasks. The Data Protection Manager shall not be dismissed or penalised by the company for performing these tasks.

	The Data Protection Manager shall directly report to the senior management level within the company.
Short term objectives	Strategically develop and improve data protection compliance ensuring the company develops a robust and effective plan for the implementation of the General Data Protection Regulations.
Long term objectives	To work with and support directorates across the company ensuring compliance with the data protection legislation. To put in place formal data protection standards - based on the supervisory authority (Data Protection Commissioner's Office) standards and legal frameworks. To inform and advise the company and its employees, who carry out data processing, of their obligations pursuant to the data protection legislation.
Main tasks	Effectively manage and administer and act as the budget holder for the Data Protection Governance financial budget. To monitor compliance with the data protection provisions, with other countries' data protection provisions and with the policies of the company in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits playing a critical role in decisions made relating to data protection. To take the lead in providing data protection advice to Members, Principal Officers, the company managers and external clients relating to all aspects of data protection. Develop and implement a comprehensive data protection plan and provide advice in this area.

	To draft complex legal agreements relating to the processing of personal information for use with external organisations in order to ensure data protection compliance, this will include but not limited to data disclosure agreements, data processing agreements, data transfer agreements, memorandum of understandings and confidentiality agreements. To provide expert advice where requested regarding data protection impact assessment process and monitor its performance. Outsourced advice is acceptable, however, Data Protection Manager must approve. To cooperate with the supervisory authority in all matters relating to information governance; and to investigate regulatory complaints in accordance with relevant regulatory requirements. To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation, and to consult, where appropriate, with regard to any other matter relating to information governance. To promote data protection compliance and best practice by setting and maintaining standards and procedures, ensuring data protection policies are up to date and disseminate any changes in the legislation to key members of staff. Oversee the management of data subject requests and data protection requests pursuant to individual rights under data protection and privacy legislation. To carry out reviews of decisions to refuse requests under the General Data Protection Regulations where required,

	whilst ensuring that the original decision made by the Information Management Officer was accurate and, where appropriate, overturn any decisions previously made. Advise on all elements of processing personal data internationally and on the requirements and implications of data protection laws. To provide detailed advice in relation to Direct Marketing specifically relating to data protection requirements and the GDPR. Where appropriate drafting a legal notice to ensure compliance with the statutory provisions, including advice relating to opt in/out clauses. To provide expert advice to the company and where appropriate draft privacy notices, fair processing notices, collection statements and any other data protection notices in order to ensure that individuals are aware of our intentions to process their data and ensuring that the company is processing personal data in a fair and lawful manner in line with the individual rights. To investigate and report on any processing, blocking, erasure, destruction and the right to be forgotten notices issued by individuals in accordance with the relevant articles contained within the GDPR, ensuring that the purposes of the processing are compatible with the conditions for processing in accordance with the Regulations and responding to the individual accordingly. Take the lead in responding to any legal claims issued against the The company for damages relating to breaches of data protection. Liaising where appropriate with the Legal Department.

	To provide expert advice in relation to any data protection queries regarding the use of social media and report any serious issues to the Chief Legal and Governance Officer. Undertake and manage data protection audits and reviews across all the company departments that are processing personal data to ensure that the company is compliant with the legislation. To manage, investigate and resolve all complaints from individuals in relation to their rights under the GDPR. Ensuring that adequate reporting mechanisms are in place for recording such complaints. Investigate breaches and incidents of data protection, establishing any potential weaknesses in the company's policies and inform the Information Governance and Security Group accordingly. Formally report all compliance issues relating to information governance, including any complaints and breaches of the legislative framework to the Chief Legal and Governance Officer/CEO/Management Board. Provide advice and assist with all data protection queries relating to projects, programmes and data sharing initiatives. Co-ordinate information governance activities with Data Protection Officers locally, regionally and nationally in relation to information management activities and attend such information governance meetings as necessary.

	In relation to the performance of these tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Outsourced Data Protection Officer (DPO)

PERSON SPECIFICATION

If a DPO is required the Data Protection Manager will be provided a budget to outsource the position.

Job title	Outsourced Data Protection Officer	
Department	Legal and Governance (Outsourced Position)	
PERSONAL ATTRIBUTES	**ESSENTIAL**	**DESIRABLE**
1. Amount of experience required	At least five years of practical work experience of dealing with data protection issues in an operational environment. Thorough understanding of the GDPR and all legislation, regulations and codes of practice relating to information governance.	Experience in conducting awareness training. Have knowledge of the current issues and general trends in the delivery of services

	Experience of developing, implementing and maintaining policies and procedures. Clear understanding of implications surrounding data protection compliance within a large organisation. High levels of communication skills, conflict management skills, relationship management skills and the characteristics and behaviours required to lead and motivate, often in times of significant pressure.	Experience of handling complaints. Experience of managing and administering a budget.
2. Technical skills required	Expert knowledge of data protection legislation, regulations and codes of conduct. Expert knowledge of the GDPR, other applicable legislation, regulations and codes of conduct. The ability to conduct investigations relating to data breaches whilst giving due consideration to the relevant Human Resource Policies in regards to GDPR.	Project management skills IT Literacy Highly proficient written, oral and presentation skills. Ability to learn new technical skills/knowledge quickly.

	Analytical and problem solving skills. The ability to interpret Information Tribunal and Court decisions. Excellent skills ownership and the ability to transfer these skills to team members where appropriate. Application of general computer software, application of specialised computer software and management systems relating to information governance.	
3. Qualifications	Educated to degree level.	GDPR Practitioner IAPP Data Protection Practitioner or demonstrable experience IAPP Freedom of Information Practitioner Complaint Investigation Training
4. Personality and Competencies	The candidate must be personable, approachable, diplomatic, tactful, enthusiastic and	

required	reliable. Must be a team player. Must be able to prioritise workload and manage multiple deadlines. Must be highly organised and ability to work under pressure. Must demonstrate a very positive attitude to the work in hand. A strong customer focus outlook and excellent communication skills. Analytical problem solver. Ability to persuade and change opinion. Good communicator, both with colleagues and customers. Highly self-motivated and directed. The ability to collect and synthesise large amounts of highly complex information, on a	

	daily basis, in order to make key decisions.	
5. Special requirements (i.e. car driver)	Drivers licence A Disclosure and Barring Service Check is an essential requirement for this post.	

DATA PROTECTION POLICY

CONTENTS

29 PURPOSE

This policy establishes an effective, accountable and transparent framework for ensuring compliance with the requirements of the GDPR.

30 SCOPE

This policy applies to all the company employees and all third parties responsible for the processing of persona data on behalf of the company services/entities.

31 POLICY STATEMENT

The company is committed to conducting its business in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of the company employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to a the company contact (i.e. the data subject).

Personal data is any information (including opinions and intentions) which relates to an identified or identifiable natural person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data. An organisation that handles personal data and makes decisions about its use is known as a Data Controller. EPM Estates, as a Data Controller, is responsible for ensuring compliance with the data protection requirements outlined in this policy. Non-compliance may expose the company to complaints, regulatory action, fines and/or reputational damage.

EPM Estates leadership is fully committed to ensuring continued and effective implementation of this policy and expects all the company employees and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

3.1. Governance

3.1.1. Data Protection Manager

To demonstrate our commitment to data protection, and to enhance the effectiveness of our compliance efforts, the company has appointed a Data Protection Manager. The Data Protection Manager operates with independence and is supported by suitability skilled individuals granted all necessary authority. The Data Protection Manager reports to THOMAS HORAN. Duties include:

- Informing and advising the company and its employees who carry out processing pursuant to data protection regulations, national law or European Union based data protection provisions;
- Ensuring the alignment of this policy with data protection regulations, national law or European Union based data protection provisions;
- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs);
- Determining the need for notifications to one or more DPAs as a result of current or intended personal data processing activities;
- Making and keeping current notifications to one or more DPAs as a result of current or intended personal data processing activities;

- The establishment and operation of a system providing prompt and appropriate responses to data subject requests;
- Informing senior managers, officers, and directors of the company of any potential corporate, civil and criminal penalties which may be levied against the company and/or its employees for violation of applicable data protection laws.

Ensuring the establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any third party who:

- provides personal data to the company service/entity
- receives personal data from the company service/entity
- has access to personal data collected or processed by the company

3.1.2. Data Protection by Design

To ensure that all data protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing. Each The company service/entity must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Data Protection Manager, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the CEO for review and approval. Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will cooperate with the Data Protection Manager to assess the impact of any new technology uses on the security of personal data.

3.1.3. Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by all the company services/entities in relation to this policy, the Data Protection Manager will carry out an annual data protection compliance audit for all such services/entities. Each audit will, as a minimum, assess:

- Compliance with the policy in relation to the protection of personal data, including:
- The assignment of responsibilities.
  - ✓ Raising awareness.
  - ✓ Training of employees.
- The effectiveness of data protection related to operational practices, including:
  - ✓ Data subject rights.
  - ✓ Personal data transfers.
  - ✓ Personal data incident management.
  - ✓ Personal data complaints handling.
  - ✓ The level of understanding of data protection policies and privacy notices.
  - ✓ The currency of data protection policies and privacy notices.
  - ✓ The accuracy of personal data being stored.
  - ✓ The conformity of data processor activities.
  - ✓ The adequacy of procedures for redressing poor compliance and personal data breaches. The Data Protection Manager, in cooperation with key business stakeholders from each the company service/entity, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies and good practice identified will be reported to, monitored and shared by the company executive team.

3.2. Data Protection Principles

The company has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data:

Principle 1: Lawfulness, Fairness and Transparency. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means, the company must tell the data subject what processing will occur (transparency), the processing must match the description given to the data subject (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).

Principle 2: Purpose Limitation. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means the company must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means the company must not store any personal data beyond what is strictly required.

Principle 4: Accuracy. Personal data shall be accurate and, kept up to date. This means the company must have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data.

Principle 5: Storage Limitation. Personal data shall be 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. This means the company must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.

Principle 6: Integrity & Confidentiality. Personal data shall be 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. The company must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

Principle 7: Accountability. The Data Controller shall be responsible for and be able to demonstrate compliance. This means the company must demonstrate that the six data protection principles (outlined above) are met for all personal data for which it is responsible.

3.3. Data collection

3.3.1. Data Sources

Personal data should be collected only from the data subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the personal data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the data subject or to prevent serious loss or injury to another person.

If personal data is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following apply:

- The data subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation
- A national law expressly provides for the collection, processing or transfer of the personal data.

Where it has been determined that notification to a data subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the personal data
- At the time of first communication if used for communication with the data subject
- At the time of disclosure if disclosed to another recipient.

3.3.2. Data subject consent

Each The company service/entity will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, the company is committed to seeking such consent. The Data Protection Manager, in cooperation with other relevant business representatives, shall establish a system for obtaining and documenting data subject consent for the collection, processing, and/or transfer of their personal data.

3.3.3. Data subject Notification

Each The company service/entity will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide data subjects with information as to the purpose of the processing of their personal data. When the data subject is asked to give consent to the processing of personal data and when any personal data is collected from the data subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The data subject already has the information;
- A legal exemption applies to the requirements for disclosure and/or consent. The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Data Protection Manager. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

3.3.4. External Privacy Notices

Each external website provided by the company will include an online ‘Privacy Notice’ and an online ‘Cookie Notice’ fulfilling the requirements of applicable law.

3.4. Data Use

3.4.1. Data processing

The company uses the personal data of its contacts for the following broad purposes:

- The general running and business administration of the company services/entities.
- To provide services to the company’s stakeholders.
- The ongoing administration and management of customer services.

The use of a contact’s information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a contact’s expectations that their details will be used by the company to respond to a contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that the company would then provide their details to third parties for marketing purposes.

Each The company service/entity will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, the company will not process personal data unless at least one of the following requirements are met:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child).

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from the Data Protection Manager before any such processing may commence.

- In any circumstance where consent has not been gained for the specific processing in question, the company will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the personal data was collected: Any link between the purpose for which the personal data was collected and the reasons for intended further processing.
- The context in which the personal data has been collected, in particular regarding the relationship between data subject and the Data Controller.
- The nature of the personal data, in particular whether special categories of data are being processed, or whether personal data related to criminal convictions and offences are being processed.
- The possible consequences of the intended further processing for the data subject.
- The existence of appropriate safeguards pertaining to further processing, which may include encryption, anonymisation or pseudonymisation.

3.4.2. Special Categories of Data

The company will only process special categories of data (also known as sensitive data) where the data subject expressly consents to such processing or where one of the following conditions apply:

- The processing relates to personal data which has already been made public by the data subject.
- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is specifically authorised or required by law.
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data or data concerning health.

In any situation where special categories of data are to be processed, prior approval must be obtained from the Data Protection Manager, and the basis for the processing clearly recorded with the personal data in question. Where special categories of data are being processed, the company will adopt additional protection measures.

3.4.3. Children's Data

Children under the age of 16 are unable to consent to the processing of personal data for information society services (any service normally provided for payment, by electronic means and at the individual request of a recipient of services). Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

3.4.4. Data Quality

Each The company service/entity will adopt all necessary measures to ensure that the personal data it collects and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the data subject. The measures adopted by the company to ensure data quality include:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification.
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required.
- Restriction, rather than deletion of personal data, insofar as:
    - ✓ a law prohibits erasure.
    - ✓ erasure would impair legitimate interests of the data subject.
    - ✓ the data subject disputes that their personal data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

3.4.5. Profiling & Automated Decision Making

The company will only engage in profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the data subject or where it is authorised by law. Where the company service/entity utilises profiling and automated decision-making, this will be disclosed to the relevant data subjects. In such cases the data subject will be given the opportunity to:

- Express their point of view.
- Obtain an explanation for the automated decision.
- Review the logic used by the automated system.
- Supplement the automated system with additional data.
- Have a human carry out a review of the automated decision.
- Contest the automated decision.

Object to the automated decision-making being carried out. Each The company service/entity must also ensure that all profiling and automated decision-making relating to a data subject is based on accurate data.

3.4.6. Digital Marketing

As a general rule the company will not send promotional or direct marketing material to an the company Contact through digital channels such as mobile phones, email and the Internet, without first obtaining their consent. Any The company service/entity wishing to carry out a digital marketing campaign without obtaining prior consent from the data subject must first have it approved by the Data Protection Manager. Where personal data processing is approved for digital marketing purposes, the data subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data processed for such purposes. If

the data subject puts forward an objection, digital marketing related processing of their personal data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted. It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

3.5. Data Retention

To ensure fair processing, personal data will not be retained by the company for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which the company services/entities need to retain personal data is set out in the Companies Data Retention Policy'. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

3.6. Data Protection

Each The company service/entity will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the personal data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data are processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can and is processed separately.
- Ensure that personal data is not kept longer than necessary

3.7. Data subject Requests

The Data Protection Manager will establish a system to enable and facilitate the exercise of data subject rights related to:

- Information access.
- Objection to processing.
- Objection to automated decision-making and profiling.
- Restriction of processing.
- Data portability.
- Data rectification.
- Data erasure. If an individual makes a request relating to any of the rights listed above

The company will consider each such request in accordance with all applicable data protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature. data

subjects are entitled to obtain, based upon a request made in writing/email to Thomas Horan <thoran@EPM Estates.ie>

It should be not ed that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights. Detailed guidance for dealing with requests from data subjects can be found in '*Data Subject Access Rights Policy and Procedure*' document.

3.8. Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If The company service/entity processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If any the company service/entity receives a request from a court or any regulatory or law enforcement authority for information relating to a the company contact, you must immediately notify the Data Protection Manager who will provide comprehensive guidance and assistance.

3.9. Data Protection Training

All The company employees that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, each the company service/entity will provide regular Data Protection training and procedural guidance for their staff.

3.10. Data Transfers

The company services/entities may transfer personal data to internal or third-party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. third countries), they must be made in compliance with an approved transfer mechanism. The company services/entities may only transfer personal data where one of the transfer scenarios lists below applies:

- The data subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the data subject
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject

3.11. Complaints handling

Data subjects with a complaint about the processing of their personal data, should put forward the matter in writing to the Data Protection Manager. An investigation of the complaint will be

carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Manager will inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the data subject and the Data Protection Manager, then the data subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

3.12. Breach Reporting

Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must immediately notify the Data Protection Manager providing a description of what occurred. Notification of the incident can be made via e-mail or by calling. The Data Protection Manager will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Data Protection Manager will follow the relevant authorised procedure based on the criticality and quantity of the personal data involved. For severe personal data breaches, the company Executive Team will initiate and chair an emergency response team to coordinate and manage the personal data breach response.

32 ROLES AND RESPONSIBILITIES

32.1 Implementation

The management team of each the company service/entity must ensure that all the company employees responsible for the processing of personal data are aware of and comply with the contents of this policy. In addition, each the company service/entity will make sure all third parties engaged to process personal data on their behalf (i.e. their data processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by EPM Estates

32.2 Support, Advice and Communication

For advice and support in relation to this policy, please contact the Data Protection Manager on email Thomas Horan <thoran@EPM Estates.ie>

33 REVIEW

This policy will be reviewed by the Data Protection Manager every three years, unless there are any changes to regulations or legislation that would enable a review earlier.

34 RECORDS MANAGEMENT

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised the company record keeping system.

All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

35 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data.

Data Processor: the entity that processes data on behalf of the Data Controller.

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union.

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

Data subject: a natural person whose personal data is processed by a controller or processor.

personal data: any information related to a natural person or 'data subject', that can be used to directly or indirectly identify the person.

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data.

Processing: any operation performed on personal data, whether by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

Regulation: a binding legislative act that must be applied in its entirety across the Union.

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

36 RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

37 FEEDBACK AND SUGGESTIONS

The company employees may provide feedback and suggestions about this document by emailing Thomas Horan <thoran@EPM Estates.ie>

DATA RETENTION POLICY

CONTENTS

38 PURPOSE

The purpose of this policy is to specify the company guidelines for retaining different types of personal data.

39 SCOPE

The scope of this policy covers all the company personal data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location. These records may be created, received or maintained in hard copy or electronically.

40 POLICY STATEMENT

40.1 The need to retain personal data varies widely with the type of data. Some personal data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. This Data Retention Policy provides guidelines to ensure that all applicable regulations and rules on personal data retention are consistently applied throughout the organisation.

Reasons for data retention

40.2 Some personal data must be retained in order to protect the company's interests, comply with regulatory requirements, preserve evidence, and generally conform to good business practices. Personal data may be retained for one or several of the following reasons:

- Business requirements
- Regulatory requirements
- Possible litigation
- Accident investigation
- Security incident investigation
- Intellectual property preservation

Retention periods

40.3 Different types of data will be retained for different periods of time:

- Personal customer data: Personal data will be held for as long as the individual is a customer of the company plus 2 years.
- Personal employee data: General employee data will be held for the duration of employment and then for 2 years after the last day of contractual employment. Employee contracts will be held for 2 years after last day of contractual employment.
- Personal tax payments will be held for 7 years.
- Records of leave will be held for 7 years.
- Recruitment details: Interview notes of unsuccessful applicants will be held for 1 year or less after interview. This personal data will then be destroyed.
- Health and Safety: 7 years for records of major accidents and dangerous occurrences unless required for legal reasons.
- Operational data: Most company data will fall in this category. Operational data will be retained for years.
- Critical data including Tax and VAT: Critical data must be retained for 7 years.

For more details, please refer to *Appendix 1 – Data Retention Schedule*

Retention of encrypted data

40.4 If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

Data duplication

40.5 When identifying and classifying EPM Estates personal data, it is important to also understand where that data may be stored, particularly for duplicate copies, so that this policy may be applied to all duplicates of the information.

Data destruction

40.6 When the retention timeframe expires, the company will actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by a member or members of the company's senior management team.
The company specifically directs users not to destroy data in violation of this policy. Destroying data that a user may feel is harmful to himself or herself or destroying data to cover up a violation of law or company policy is particularly forbidden.

41 RESPONSIBILITIES

Compliance, monitoring and review

41.1 The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing data transfer activities at the company rests with the Data Protection Manager.

41.2 All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant the company policies and procedures.

Reporting in case of a data breach

41.3 In the case of possible data breach, the staff member(s) who first identifies the breach or incident, must immediately report all details of the incident to the Data Protection Manager.

41.4 The Data Protection Manager is required to report a personal data breach to the competent Data Protection Authority not later than 72 hours after becoming aware of it. The notification must include at least:

- a description of the nature of the breach, including, where possible, the categories and approximate number of data subjects and personal data records concerned;
- the name and contact details of the relevant Data Protection Manager or contact point;
- the likely consequences of the data breach; and
- measures taken or proposed by the controller to address the breach and/or mitigate its effects.

41.5 Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the Data Protection Manager must communicate the breach to the data subject(s) without undue delay. The communication must describe in clear and plain language, the nature of the breach and at least:

- the name and contact details of the relevant Data Protection Manager or contact point;
- the likely consequences of the data breach; and
- measures taken or proposed by the controller to address the breach and/or mitigate its effects.

Records management

41.6 Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised the company recordkeeping system.

41.7 All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

42 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Manager (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Processing: any operation performed on personal data, whether by automated means, including collection, use, recording, etc.

Data Backup: data copied to a second location, solely for the purpose of safe keeping of that data

Data Encryption: the process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored

Data Encryption Key: an alphanumeric series of characters that enables data to be encrypted and decrypted

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

43 RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- The companyData Protection Policy

44 FEEDBACK AND SUGGESTIONS

44.1 The company employees may provide feedback and suggestions about this document by emailing Thomas Horan <thoran@EPM Estates.ie>.

45 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Thomas Horan
Data Protection Manager	Thomas Horan
Next Review Date	15/10/2022

DATA SECURITY POLICY

CONTENTS

PURPOSE

This policy establishes an effective, accountable and transparent framework for ensuring high standards of data security at EPM Estates.

SCOPE

This policy applies across all entities or subsidiaries owned, controlled, or operated by and to all employees, including part-time, temporary, or contract employees.

POLICY STATEMENT

Physical security

The The companyoffice is under strong security protection, at both premises level and floor level to ensure only authorized individuals have access to the building and the company office. At the premises level, the building's perimeter is secured by barriers and/or locks. At the floor level employees are granted access to the office only after authorization. Critical locations in the office are accessible only to authorized individuals.

Important documents are stored in cabinets that can only be accessed by pre-authorized individuals. The office may be equipped with surveillance cameras and their footage is monitored periodically by authorized individuals. Fire alarms and water sprinklers are in place to detect and mitigate damage in the unlikely event of a fire. Regular fire drills are also conducted by the premises management team to educate employees about emergency evacuation procedures. A policy has been implemented to approve and regulate visitor access to the building. The office is provided with 24x7 power supply, supported by an alternative uninterrupted power supply system to ensure smooth functioning in the event of power failure.

The companyhosts its application and data in industry-leading Cloud Services, whose data centers have been thoroughly tested for security, availability and business continuity.

Application security

All of EPM Estates applications are up to date and secure. The infrastructure for databases and application servers is managed and maintained by certified and/or qualified personal or agents.

At EPM Estates, we take a multifaceted approach to application security, to ensure everything from engineering to deployment, including architecture and quality assurance processes complies with our highest standards of security.

Application Architecture

The application is initially protected by certified and/or qualified personal or agents' firewall which is equipped to counter regular DDoS attacks and other network related intrusions. The second layer of protection is the company own application firewall which monitors against offending IPs, users and spam. While the application can be accessed only by users with valid credentials, it should be noted that security is a shared responsibility between the company and the businesses who own those accounts on the cloud. In addition to making it easy for administrators to enforce industry-standard password policies on users, our applications also incorporate features aimed at securing business data on the cloud:

- Configuring secure socket connections to portals;
- Leveraging SAML and custom single sign-on;
- Whitelisting IPs for exclusive access;
- Identity management via Google and Facebook credentials;
- Custom email servers, etc.;
- It should be noted that all account passwords that are stored in the application are one-way hashed and salted.

The companyuses a multi-tenant data model to host all its applications. Each application is serviced from an individual virtual private cloud and each customer is uniquely identified by a tenant ID. The application is engineered and verified to ensure that it always fetches data only for the logged-in tenant. Per this design, no customer has access to another customer's data. Access to the application by the The companydevelopment team is also controlled, managed and audited. Access to the application and the infrastructure are logged for subsequent audits.

The in-line email attachment URLs for the product are public by design, to enable us to embed links within the email for end-user ease. This can be made private on customer request.

Application Engineering and Development

Our engineers or agents are trained in industry-leading secure coding standards and guidelines to ensure our products are developed with security considerations from the ground-up. A security review is a mandatory part of application engineering process at EPM Estates. The security review leverages static code analysis tools, in addition to manual reviews, to ensure adherence to our highest standards.

Quality Assurance

Besides functional validation and verification, the quality assurance process at The company also subjects application updates to a thorough security validation. The validation process is performed by a dedicated app security team with ethical hackers whose goal is to discover and demonstrate vulnerabilities in the application. An update to the application does not get the stamp of approval from the quality assurance team if vulnerabilities (that can compromise either the application or data) are identified.

Data Security

The company takes the protection and security of its customers' data very seriously. The company manages the security of its application and customers' data. However, provisioning and access management of individual accounts is at the discretion of individual business owners.

The The company development team has no access to data on production servers. Changes to the application, infrastructure, web content and deployment processes are documented extensively as part of an internal change control process.

Our products collect limited information about customers - name, email address and phone - which are retained for account creation. Postal address is requested and retained by The company PCI compliant payment processor for billing, along with the date of expiry of credit card and CVV.

The company takes the integrity and protection of customers' data very seriously. We maintain history of two kinds of data: application logs from the system, and application and customers' data..

Application logs are maintained for a duration of 90 days. Customers' data is backed up in two ways:

1 A continuous backup is maintained in different data center's to support a system failover if it were to occur in the primary data center. Should an unlikely catastrophe occur in one of the data center's, businesses would lose only five minutes of data.

f) Data is backed up to persistent storage every day and retained for the last seven days.

The data at rest is encrypted using AES 256bit standards (key strength - 1024). All data in transit is encrypted using FIPS-140-2 standard encryption over a secure socket connection for all accounts hosted on Cloud Services.com. For accounts hosted on independent domains, an option to enable a secure socket connection is available.

Different environments are in use for development and testing purposes, access to systems are strictly managed, based on the principles of need to do/know basis appropriate to the information classification, with Segregation of Duties built in, and reviewed on a quarterly basis.

Data Deletion

When an account is deleted, all associated data is destroyed within 14 business days. The company products also offer data export options which businesses can use if they want a backup of their data before deletion.

Operational Security

The company understands that formal procedures, controls and well-defined responsibilities need to be in place to ensure continued data security and integrity. The company has clear change management processes, logging and monitoring procedures, and fall back mechanisms which have been set up as part of its operational security directives.

Operational security starts right from recruiting an engineer to training and auditing their work products. The recruitment process includes standard background verification checks (including verification of academic records) on all new recruits. All employees are provided with adequate training about the information security policies of the company and may be required to sign that

They have read and understood the company's security-related policies. Confidential information about the company is available for access only to select authorized the company employees.

Employees are required to report any observed suspicious activities or threats. The human resources team takes appropriate disciplinary action against employees who violate organizational security policies. Security incidents (breaches and potential vulnerabilities) can be reported by emailing Thomas Horan <thoran@EPM Estates.ie>

The company maintains an inventory of all information systems used by employees for development purposes in an internal service desk, aided by automated probing software that assists in tracking changes to these systems and their configurations. Only authorized and licensed software products are installed by employees. No third parties or contractors manage software or information facilities, and no development activity is outsourced. All employee information systems are authorized by the management before they are installed or put to use.

In order to test the resilience of the hosted application, the company employs an external security consultant and additional ethical hackers who perform penetration tests. This is always conducted in an architecturally equivalent copy of the system with no actual customer data present. The production system is never subject to such tests. Should an individual attempt such a test in the production environment, it will be detected as an intrusion, and the source IP will be blocked. An alert will then be raised so engineers can attend to the incident.

The company has a *Data Protection Policy*, approved by the senior management.

Network Security

Network security is discussed in detail in this section from the perspective of the development center, and the network where the application is hosted.

The company office network where updates are developed, deployed, monitored and managed is secured by industry-grade firewalls and antivirus software, to protect internal information systems from intrusion and to provide active alerts in the event of a threat or an incident. Firewall logs are stored and reviewed periodically. Access to the production environment is via SSH and remote access is possible only via the office network. Audit logs are generated for each remote user session and reviewed. Also, the access to production systems are always through a multi-factor authentication mechanism.

All the company products are hosted in securely, with security managed by certified and/or qualified personal or agents. Our team monitors the infrastructure for stability, intrusions and spam using a dedicated alert system. Every three months, end-to-end vulnerability assessments and penetration tests are performed. The company application has an in- built spam protection system for businesses that use it, while our team monitors and blocks individual accounts and IP addresses which attempt to access the company applications.

RESPONSIBILITIES

Regulatory Compliance

All formal processes and security standards at The company are designed to meet regulations at the industry, state and European Union levels.

Use of our service by customers in the European Economic Area ("EEA"), will include the processing of information relating to their customers. In providing our service, we do not own, control or direct the use of the information stored or processed on our platform at the direction of our customers, and in fact we are largely unaware of what information is being stored on our platform and only access such information as reasonably necessary to provide the service (including to respond to support requests), as otherwise authorized by our customers or as required by law. We are Data Processors for our end customers, but Data Controllers for the customers from whom we collect data on our platform for purposes of the European Union ("EU") on our platform for purposes of the European Union ("EU") General Data Protection Regulation (GDPR). Our EEA based customers, who control their customer data and send it to The company for processing, are the "Controllers" of that data and are responsible for compliance with the GDPR. In particular, The company customers are responsible for complying with the GDPR and relevant data protection legislation in the relevant EEA member state before sending personal information to The company for processing.

As the processors of personal information on behalf of our customers, we follow their instructions with respect to the information they control to the extent consistent with the functionality of our service. In doing so, we implement industry standard security, technical, physical and administrative measures against unauthorized processing of such information and against loss, destruction of, or damage to, personal information as more fully described in EPM Estates Project's Data Protection Policy.

We work with our customers to help them provide notice to their customers concerning the purpose for which personal information is collected and sign Standard Data Processor Agreement (for data processors) with them to legitimize transfers of personal data from EU to processors established in third countries as may be required under the GDPR.

Reporting issues and threats

If you have found any issues or flaws impacting the data security or privacy of The company users, please email Thomas Horan <thoran@EPM Estates.ie> with the relevant information so we can get working on it right away.

Your request will be looked into immediately. We might ask for your guidance in identifying or replicating the issue and understanding any means to resolving the threat right away. Please be clear and specific about any information you give us. We deeply appreciate your help in detecting and fixing and will acknowledge your contribution to the world once the threat is resolved.

Records management

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognized The company record keeping system.

All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Manager (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyze, or predict data subject behavior

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

RELATED LEGISLATION AND DOCUMENTS

- ☐ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- ☐ The companyData Protection Policy

FEEDBACK AND SUGGESTIONS

- The company employees may provide feedback and suggestions about this document by emailing Thomas Horan <thoran@EPM Estates.ie>.

APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Thomas Horan
Data Protection Manager	Thomas Horan
Next Review Date	15.10.2022

DATA TRANSFERS POLICY

CONTENTS

PURPOSE

This policy and procedure establishes an effective, accountable and transparent framework for ensuring compliance with the requirements for data transfers by the GDPR.

SCOPE

This policy and procedure applies across all entities or subsidiaries owned, controlled, or operated by the company and to all employees, including part-time, temporary, or contract employees, that handle personal data and/or personal data transfers.

POLICY STATEMENT

The company services/entities may transfer personal data to internal or third-party recipients located in another country where that country or third-party is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. third countries), they must be made in compliance with an approved transfer mechanism. The company services/entities may only transfer personal data where one of the transfer scenarios lists below applies:

- The data subject has given consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the data subject
- The transfer is necessary for the implementation of pre-contractual measures taken in
- response to the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary to protect the vital interests of the data subject

Transfers between the company services/entities

In order for the company to carry out its operations effectively across its various services/entities, there may be occasions when it is necessary to transfer personal data internally from one Entity to another or to allow access to the personal data from an overseas location. Should this occur, the company service/entity sending the personal data remains responsible for ensuring protection for that personal data.

The company handles the transfer of personal data between the company services/entities, where the location of the recipient entity is a third country, using the binding corporate rules transfer mechanism. Binding corporate rules provide legally binding, enforceable rights on data subjects with regard to the processing of their personal data and must be enforced by each approved the company service/entity, including their employees. Only transfer the minimum amount of personal data necessary for the particular purpose of the transfer (for example, to fulfil a transaction or carry out a particular service). Ensure adequate security measures are used to protect the personal data during the transfer (including password-protection and encryption, where necessary).

Transfers to Third Parties

Each of the company service/entity will only transfer personal data to, or allow access by, third parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where third party processing takes place, each the company service/entity will first identify if, under applicable law, the third party is considered a data controller, or a data processor of the personal data being transferred.

Where the third party is deemed to be a data controller, the company service/entity will enter into, in cooperation with the Data Protection Manager, an appropriate agreement with the controller to clarify each party's responsibilities in respect to the personal data transferred. Where the third party is deemed to be a data processor, the company service/entity will enter into, in cooperation with the Data Protection Manager, an adequate processing agreement with the data processor. The agreement must require the data processor to protect the personal data from further disclosure and to only process personal data in compliance with the company instructions. In addition, the agreement will require the data processor to implement appropriate technical and organisational measures to protect the personal data as well as procedures for providing notification of personal data breaches.

The company has a 'Standard Data Processing Agreement' document that, should be used as a baseline template. When the company service/entity is outsourcing services to a third party (including cloud computing services), they will identify whether the third party will process personal data on its behalf and whether the outsourcing will entail any third country transfers of personal data. In either case, it will make sure to include, in cooperation with the company Data Protection Manager, adequate provisions in the outsourcing agreement for such processing and third country transfers.

RESPONSIBILITIES

Compliance, monitoring and review

The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing data transfers activities at the company rests with the Data Protection Manager.

All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant the company policies and procedures.

Records management

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised the company record-keeping system.

All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Manager (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation: a binding legislative act that must be applied in its entirety across the Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

RELATED LEGISLATION AND DOCUMENTS

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- The company Data Protection Policy

FEEDBACK AND SUGGESTIONS

45.1 The company employees may provide feedback and suggestions about this document by emailing Thomas Horan <thoran@EPM Estates.ie>

APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Thomas Horan
Data Protection Manager	Thomas Horan
Next Review Date	15.10.2022

Due Diligence Letter

DATE
RECIPIENT NAME
ADDRESS

Dear Sir/Madam

The company is currently contacting all suppliers of services to our company for the purposes of performing a due diligence check in regard to the new General Data Protection Regulation due to come into force on the on the 25th May 2018.

Please note that as per Article 28(1) of the GDPR we can only use a supplier (Data Processor) who is "**providing sufficient guarantees to implement appropriate technical or organisation measures, in such a manner that processing will meet the requirements of this regulation…".** Therefore, we have compiled a supplier questionnaire (see attached) which we would like your organisation to complete and return to the company. We will carefully review responses from suppliers and make decisions in the very near future, so a reply as soon as possible would be appreciated.

If we are within an extended period contract, which extends beyond 25th May 2018, we will still require a response to the questions attached as well as confirmation that the terms and conditions, on the existing contract, will be amended to contain the specific data privacy wording required by the GDRP legislation, to clarify your organisations obligations and duties to the company under the new legislation.

Thank you,

Thomas Horan <thoran@EPM Estates.ie>
The company

Data Processor Checklist

Please complete and return to email address Thomas Horan <thoran@EPM Estates.ie>

Name of supplier:
Main supplier contact details for all data privacy matters:

REQUIREMENT	YES/NO	COMMENT
Please confirm what enough guarantees you can give the company that demonstrate your understanding and implementation of your obligation, as a processor, under the new GDPR legislation, including any certifications or externally audited processes.		
Do your standard contract terms include the new GDPR mandatory provisions?		
Do your standard contract terms propagate down, within a formal contract, to your sub contract providers involved in the service to EPM Estates?		
Are you maintaining Data Processing Records? (as outlined in Article 30 of GDPR)		
Please detail all sub-contractors, included in the provision of your service to EPM Estates		
Do you have a documented Breach Notification Process to ensure notification to the company within 72hrs?		
Do you and your sub processors, providing the service to EPM Estates, have a documented process for the deletion of subject's records, upon request, from both live or archived records and backups of your systems?		
Can you confirm our right to have personal data deleted or upon termination of contract at no extra cost?		
Does yours and your sub processor/s, involved in the delivery of services to EPM Estates, website/software have a data privacy policy and fair processing notice which meet GDPR requirements?		
Do your contracts of employment contain confidentiality and gross misconduct clauses, in the context of customers data privacy?		

Privacy Notice

Introduction

This document refers to personal data, which is defined as information concerning any living person (a natural person who hereafter will be called the Data Subject) that is not already in the public domain.

The General Data Protection Regulation (GDPR) seeks to protect and enhance the rights of data subjects. These rights cover the safeguarding of personal data, protection against the unlawful processing of personal data and the unrestricted movement of personal data within the EU. It should be noted that GDPR does not apply to information already in the public domain.

The EPM Estates is pleased to provide the following Privacy Notice:

Personal Data

The EPM Estates uses the information collected from you to provide quotations, make telephone contact and to email you marketing information which we believe may be of interest to you and your business. In you making initial contact you consent to EPM Estates maintaining a marketing dialogue with you until you either opt out (which you can do at any stage) or we decide to desist in promoting our services. The EPM Estates also acts on behalf of its clients in the capacity of data processor. When working exclusively as a data processor, The EPM Estates will be acting on the instruction of its client, and will work hard to ensure that the client is fully GDPR compliant.

Some personal data may be collected about you from the forms and surveys you complete, from records of our correspondence and phone calls and details of your visits to our website, including but not limited to personally identifying information like Internet Protocol (IP) addresses. EPM Estates from time to time may use such information to identify its visitors. EPM Estates may also collect statistics about the behavior of visitors to its website.

The company website uses cookies, which is a string of information that a website stores on a visitor's computer, and that the visitor's browser provides to the website each time the visitor returns. WordPress.org uses cookies to help The Company identify and track visitors and their website access preferences. EPM Estates website visitors who do not wish to have cookies placed on their computers should set their browsers to refuse cookies before using EPM Estates website.

Any information EPM Estates about you and your business encompasses all the details we hold about you and any sales transactions including any third-party information we have obtained about you from public sources and our own suppliers such as credit referencing agencies.

EPM Estates only collect the information needed so that it can provide you with marketing and consulting services; this agency does not sell or broker your data, although coincidentally there may be times when your information could be contained in data that EPM Estates has purchased from a third-party list broker, on behalf of a client.

Legal basis for processing any personal data

To meet The company contractual obligations to clients and to also respond to marketing enquiries.

Legitimate interests pursued by the company and/or its clients

To promote the marketing and consulting services offered EPM Estates and/or to market the services and/or products offered by EPM Estates existing clients.

Consent

Through agreeing to this privacy notice you are consenting to EPM Estates processing your personal data for the purposes outlined. You can withdraw consent at any time by emailing Thomas Horan <thoran@EPM Estates.ie> or writing to us, see last section for full contact details.

Disclosure

EPM Estates may on occasions pass your Personal Information to third parties exclusively to process work on its behalf. EPM Estates requires these parties to agree to process this information based on our instructions and requirements consistent with this Privacy Notice and GDPR.

EPM Estates do not broker or pass on information gained from your engagement with the agency without your consent. However, EPM Estates may disclose your Personal Information to meet legal obligations, regulations or valid governmental request. The agency may also enforce its Terms and Conditions, including investigating potential violations of its Terms and Conditions to detect, prevent or mitigate fraud or security or technical issues; or to protect against imminent harm to the rights, property or safety of EPM Estates, its clients and/or the wider community.

Retention Policy

EPM Estates will process personal data during the duration of any contract and will continue to store only the personal data needed for five years after the contract has expired to meet any legal obligations. After five years any personal data not needed will be deleted.

Data storage

EPM Estates does not store personal data outside the EEA without prior consent or approved transfer guidance under the GDPR such as a Privacy Shield.

Your rights as a data subject:

At any point whilst The company is in possession of or processing your personal data, all data subjects have the following rights:

- ☐ **Right of access** – you have the right to request a copy of the information that we hold about you.
- ☐ **Right of rectification** – you have a right to correct data that we hold about you that is inaccurate or incomplete.

- ☐ **Right to be forgotten** – in certain circumstances you can ask for the data we hold about you to be erased from our records.
- ☐ **Right to restriction of processing** – where certain conditions apply you have a right to restrict the processing.
- ☐ **Right of portability** – you have the right to have the data we hold about you transferred to another organization.
- ☐ **Right to object** – you have the right to object to certain types of processing such as direct marketing.
- ☐ **Right to object to automated processing, including profiling** – you also have the right not to be subject to the legal effects of automated processing or profiling.

In the event that The company refuses your request under rights of access, we will provide you with a reason as to why, which you have the right to legally challenge.

The company at your request can confirm what information it holds about you and how it is processed

You can request the following information:

- ☐ Identity and the contact details of the person or organisation (EPM Estates) that has determined how and why to process your data.
- ☐ Contact details of the Data Protection Manager, where applicable.
- ☐ The purpose of the processing as well as the legal basis for processing.
- ☐ If the processing is based on the legitimate interests of the company or a third party such as one of its clients, information about those interests.
- ☐ The categories of personal data collected, stored and processed.
- ☐ Recipient(s) or categories of recipients that the data is/will be disclosed to.
- ☐ How long the data will be stored.
- ☐ Details of your rights to correct, erase, restrict or object to such processing.
- ☐ Information about your right to withdraw consent at any time.
- ☐ How to lodge a complaint with the supervisory authority (Data Protection Regulator).
- ☐ Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether you are obliged to provide the personal data and the possible consequences of failing to provide such data.
- ☐ The source of personal data if it wasn't collected directly from you.
- ☐ Any details and information of automated decision making, such as profiling, and any meaningful information about the logic involved, as well as the significance and expected consequences of such processing.

To access what personal data is held, identification will be required

The companywill accept the following forms of ID when information on your personal data is requested: a copy of your national ID card, driving license, passport, birth certificate and a utility bill not older than three months. A minimum of one piece of photographic ID listed above and a supporting document is required. If The companyis dissatisfied with the quality, further information may be sought before personal data can be released.

All requests should be made to Thomas Horan <thoran@EPM Estates.ie> or by phoning or writing to us at the address further below.

Complaints

In the event that you wish to make a complaint about how your personal data is being processed by The Company or its partners, you have the right to complain to EPM Estates. If you do not get a response within 30 days, you can complain to the Data Protection Regulator.

The details for each of these contacts are:

EPM Estates, attention of Thomas Horan <thoran@EPM Estates.ie>
Unit 3 JFK House,
John F Kennedy Road,
Bluebell, Dublin 12. D12 C966

Data Protection Regulator:

Helen Dixon

Canal House
Station Road,
Portarlington,
Co. Laois,
R32 AP23,
Ireland
Telephone +353 (0761) 104 800 or email: info@dataprotection.ie

SUBJECT ACCESS REQUEST FORM

If you want us to supply you with a copy of any personal data we hold about you, please complete this form and send it the address below. You are currently entitled to receive this information under the EU General Data Protection Regulation (GDPR). We will also provide you with information about any processing of your personal data that is being carried out, the retention periods which apply to your personal data, and any rights to rectification, erasure, or restriction of processing that may exist.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to your request.

Please send your completed form and proof of identity to:

EPM Estates
Head Office,
Unit 3 JFK House,
John F Kennedy Road,
Bluebell, Dublin 12. D12 C966

Section 1: Details of the person requesting information

Your full name:	
Your address:	
Your telephone number:	
Your email address:	

Section 2: Are you the data subject?

Please tick the appropriate box.

☐ **YES**: I am the data subject. I enclose proof of my identity (see below). Please proceed to Section 4.

☐ **NO**: I am acting on behalf of the data subject. I have enclosed the data subject's written authority and proof of the data subject's identity and my own identity (see below). Please proceed to Section 3.

To ensure we are releasing data to the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one of both of the following:

1) **Proof of Identity.** We need one of the following: passport, photo driving license, national identity card, birth certificate.
2) **Proof of Address.** We need one of the following: utility bill, bank statement, credit card statement (no more than 3 months old); current driving license; local authority tax bill.

If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

Section 3: Details of the data subject

Your full name:	
Your address:	
Your telephone number:	
Your email address:	

Section 4: What information are you seeking?

Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require.

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

Please note that if the information you request reveals details directly or indirectly about another person we will have to seek the consent of that person before we can let you see that information. In certain circumstances, where disclosure would adversely affect the rights and freedoms of

others, we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision.

While in most cases we will be happy to provide you with copies of the information you request, we nevertheless reserve the right, in accordance with Article 12 of the GDPR to charge a fee or refuse the request if it is considered to be "manifestly unfounded or excessive". However, we will make every effort to provide you with a satisfactory form of access or summary of information if suitable.

Section 5: Information about the data collection and processing

If you want information about any of the following, please tick the boxes:

☐ Why we are processing your personal data

☐ To whom your personal data are disclosed

☐ The source of your personal data

46 Section 6: Disclosure of CCTV images

If the information you seek is in the form of video images captured by our CCTV security cameras, would you be satisfied with viewing these images?

☐ **YES**

☐ **NO**

Section 7: Declaration

Please note that any attempt to mislead may result in legal action.

I confirm that I have read and understood the terms of this Data Subject Access Request Form and certify that the information given in this application to the company is true. I understand that it is necessary for the company to confirm my / the data subject's identity and it may be necessary to obtain more detailed information to locate the correct personal data.

……..

……

Signature Date

47 Attachments:

I am enclosing the following copies as proof of identity:

……

……

……

……

……

.....
.....
.....
.....
.....

Cookie Policy

What is a cookie?

A cookie is a small text file that may be stored on your computer or mobile device that contains data related to a website you visit. It may allow a website "remember" your actions or preferences over a period of time, or it may contain data related to the function or delivery of the site. Cookies can be set by the owner of the website or in some cases by third party services the website owner allows to present other information, run content or provide other functionality such as analytics.

Further information on cookies can be found at: http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm
How are they used on this site?

EPM Estates uses cookies only for functionality that is strictly necessary for services that are explicitly requested by the user for their session as per Regulation 5(5), SI 336 of 2011 (the ePrivacy Regulations).

This website uses session cookies. Session cookies are used to deliver the basic functions of a website i.e. to allow pages to remember technical changes or selections you may make between pages. Session cookies are temporary cookies and are generally erased when you close your browser.

We use a session cookie to remember your language preference when viewing the site. This session cookie (called USERLANG) is erased when you close your browser or after 5 minutes of inactivity.

EPM Estates does not use any third party or persistent cookies without first receiving concent.

Managing Cookies
Within your browser you can choose whether you wish to accept cookies or not. Different browsers make different controls available to you and so we provide links below to popular manufacturers' instructions on how you can do this. Generally, your browser will offer you the choice to accept, refuse or delete cookies at all times, or those from providers that website owners use ("third party cookies"), or those from specific websites.

· Google Chrome
· Internet Explorer

· Firefox
· Safari
· Safari Mobile
· Opera

This Cookie Policy forms part of our overall Privacy Statement

Staff Privacy Agreement

This statement explains how the company handles and uses personal data we collect about staff. Where in this statement we refer to 'we' or 'our' or 'us' we are referring to the company and where we refer to 'you' or 'your' we are referring to our staff.

We are committed to protecting your personal information and to being transparent about what information we hold. The company understands its obligations to you to help you understand how and why we process your personal data. This notice tells you about these uses and should be read in conjunction with the company data protection policy as found on the company website.

Our data protection policy and procedures are governed by the Data Protection Act 1998 and, from 25th May 2018, the EU General Data Protection Regulation. The law in this area is changing rapidly and we anticipate this statement may be revised in line with guidance from the Information Commissioner's office.

Why we hold your personal data

We are required to hold your personal data for various legal and practical purposes, without which we would be unable to employ you.

Holding your personal data enables us to meet various administrative and legal obligations (eg for tax purposes).

We will also process your personal information in other circumstances, provided you have given your consent for us to do so.

Lawful basis for processing personal data

The lawful basis for processing the staff personal data as described in this document is to fulfil a contract with an individual.

There is a contractual requirement for you to provide much of the information detailed. Without this we will be unable to fulfil our obligations which could result in the contract terminating.

The company may also store some of your personal data in accordance with other privacy notices (Staff Training and/or events).

Personal data held by EPM Estates

The information we hold about you is primarily information you provided when applying for your job, supplemented by information generated in the course of your employment.

In common with all data subjects:

□ Your name Your contact details Unique personal identifiers and biographical information (e.g. date of birth) photographs of you; your attendance at The company events; personal data provided by you for a specific purpose or purposes (for example, disability, catering preferences or lifestyle status for event management); information related to the prevention and detection of crime and the safety of staff including, but not limited to, CCTV recording;

Also: financial information gathered for the purposes of administering payroll.

Particular to staff: your application and curriculum vitae; details of your career; references. your contract of employment; performance reviews; disciplinary, grievance and capability procedures; accidents at work; and training provided.

Sensitive personal data held by EPM Estates

The information we hold is that which you provide to us (for example, you may give us information by filling in forms on our website, or by corresponding with us by post, telephone, email or otherwise).

How your personal data is used by EPM Estates

Your data is used by us for a number of purposes including:

All data subjects: Publications, invitations and other communications. e-news and flash emails. internal reporting and record keeping. the promotion of staff events. administrative purposes (e.g. in order to process fees payments or to administer an event you have registered for or attended). Responding to data access requests you make.

Communications to you may be sent by post, telephone or a work email address. Your personal mobile phone number will only be used if you have given consent.

If you have concerns or queries about any of these purposes, or how we communicate with you, please contact us at the address given below. We will always respect a request by you to stop processing your personal data, and in addition your statutory rights are set out below.

Sharing your data with others

Within EPM Estates, personal data, including sensitive personal data, may be shared between members of staff, including Trustees, who legitimately need the information to carry out their normal duties to support your time with us. We endeavour to ensure that sensitive personal data is only shared with colleagues with your explicit consent. However, circumstances may arise where this data is shared with colleagues without gaining your consent. This will only occur if it is necessary to protect your vital interests or the vital interests of another person; or for certain other reasons where it is not possible or appropriate to gain your consent such as disclosures to the authorities for prevention or detection of crime, or to meet statutory obligations relating to equality monitoring. The company may disclose certain personal data to third parties. These external organisations, and the purpose for sharing the information, are set out below.

Relevant data, including your bank details, will be shared with our payroll providers and may be shared with our accountants (for payment of expenses).

Relevant data may be shared with your next of kin but only with your consent or in an emergency.

Relevant data may be shared with Home Office, Irish Visas and Immigration in order to fulfil our obligations as a visa sponsor.

Data may be shared with reputable “data processors” for the purposes of sending communications (eg mailchimp).

With your permission we may share information about you for publicity and marketing purposes online, in print and on social media.

Otherwise, the company does not share data with any third party, except as allowed for in other privacy notices or required by law. We do not sell your personal data to third parties under any circumstances or permit third parties to sell on the data we have shared with them.

Transfer of personal data to other countries Where data is shared within the EAA, or the European Union (EU), the third party will be required to comply with and safeguard the data under the terms of the GDPR EU regulations.

Your personal information will only be transferred to countries, outside of the EU, whose data protection laws have been assessed as adequate by the European Commission, or where adequate safeguards, such as the EU-US Privacy Shield, are in place.

How long data is kept We will keep your personal data only as long as is necessary for the purpose(s) for which it was collected, and in accordance with our Data Protection Policy. Data will be securely destroyed when no longer required.

Where you exercise your right to erasure, we will continue to maintain a core set of personal data (name, dates of working at the company and date of birth) to ensure we do not contact you inadvertently in future, and to maintain your record for archive purposes. We may also need to retain some financial records about you for statutory purposes (e.g. accounting matters).

Your rights

You have the following rights

To be informed This Privacy Notice provides the information you are entitled to receive Access Please contact us if you would like confirmation that your data is being processed and access to your personal data.

There is no charge for us providing you with this data and it will usually be provided within a month of the request (unless the request is unfounded or excessive). Rectification Please inform us of any data which you would like rectified and we will usually respond within a month of the request.

We will pass on the changes to any third parties who need to change their records and let you know this has been done. Erasure You may exercise your right to have your personal data erased in a number of circumstances (eg if the data is no longer necessary in relation to the purpose for which it was created, or you withdraw your consent). Where possible we will comply with all such requests, though some details are part of the College's permanent records (eg examination results, college photographs) which cannot reasonably be deleted. Restrict processing You can tell us that we can keep your data but must stop processing it, including preventing future mailings and communications.

If possible, we will inform any third parties to whom your data has been disclosed of your requirement. Data portability Your data is across manual records and a bespoke Access database. We will do our best to provide information in a portable format, but it is unlikely that we can create systems to do so. to object If we can, we will stop processing your data if you object to processing based on legitimate interests or the performance of a task in the public interest / exercise of official authority (including profiling).

We will stop processing your data for direct marketing if you tell us to.

We will stop processing your data if you object to processing for purposes of research and statistics.

Not to be subject to automated decision-making including profiling

We do not use any automated decision-making.

We reserve the right to judge what information we must continue to hold to be able to fulfil our contract with you.

You have the right to lodge a complaint with the Irish Data Protection Commissioner's Office at https://www.dataprotection.ie/docs/Home/4.htm.

Further information

Our Data Protection Manager is responsible for monitoring compliance with relevant legislation in relation to the protection of personal data. Please contact Thomas Horan <thoran@EPM Estates.ie> if you have any concerns or questions about the above information or you wish to ask us not to process your personal data for particular purposes or to erase your data. Where you have specific requests relating to how we manage your data, we will endeavor to resolve these, but please note that there may be circumstances where we cannot comply with specific requests.

If you have any concerns about your personal data held by the company, you will need to contact please contact our Data Protection Manager at the details provided above.

Clean Desk Policy

Overview

The company stands committed to the development of secure policies and practices, and in doing so, has implemented this Clean Desk Policy to increase physical security at the company locations. This policy ensures that confidential information and sensitive materials are stored away and out of sight when they are not in use or when the workspace is vacant.

This policy sets forth the basic requirements for keeping a clean workspace, where sensitive and confidential information about the company employees, clients, vendors, and intellectual property is secured.

The policy shall apply to all the company employees, contractors, and affiliates.

Policy

1. Employees are required to secure all sensitive/confidential information in their workspace at the conclusion of the work day and when they are expected to be away from their workspace for an extended period of time. This includes both electronic and physical hardcopy information.
2. Computer workstations/laptops must be locked (logged out or shut down) when unattended and at the end of the work day. Portable devices like laptops and tablets that remain in the office overnight must be shut down and stored away.
3. Mass storage devices such as CD, DVD, USB drives, or external hard drives must be treated as sensitive material and locked away when not in use.
4. Printed materials must be immediately removed from printers or fax machines. Printing physical copies should be reserved for moments of absolute necessity. Documents should be viewed, shared and managed electronically whenever possible.
5. All sensitive documents and restricted information must be placed in the designated shredder bins for destruction or placed in the locked confidential disposal bins. Please refer to the Records Retention Policy for additional information pertaining to document destruction.
6. File cabinets and drawers containing sensitive information must be kept closed and locked when unattended and not in use.

7. Passwords must not be written down or stored anywhere in the office.
8. Keys and physical access cards must not be left unattended anywhere in the office.

It is the responsibility of Thomas Horan to ensure enforcement with the policies above. Repeated or serious violations of the clean desk policy can result in disciplinary actions in accordance with the Company Employee Handbook.

If you notice that any of your devices or documents have gone missing, or if you believe your workspace has been tampered with in any way, please notify Thomas Horan <thoran@EPM Estates.ie> immediately**.**