JPR environmental

The Malthouse, Standish, Stonehouse
Gloucestershire GL10 3DL
T. 01453 822584

DATA PROTECTION POLICY

Introduction

JPR Environmental is required to comply with the law governing the management and storage of personal data, which is outlined in the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Data protection and GDPR compliance is overseen by the UK supervisory authority which is the Information Commissioner's Office (ICO). JPR Environmental is accountable to the ICO for all of its data protection compliance.

Protection of personal data and respect for individual privacy and the rights of data subjects are fundamental to the day-to-day operations of JPR Environmental.

Purpose of this policy

This policy is applicable to everyone working for and with JPR Environmental and aims to protect and promote the data protection rights of every individual whose data we process.

Scope of the policy

This policy applies to all members, staff, consultants and any third party to whom this policy has been communicated. It covers all personal data and special categories of personal data under GDPR, regardless of where or how it is stored, e.g. hard copy or digital, mobile or fixed device - see below for further explanations and definitions of data types.

Responsibility

Everyone working for and with the organisation is responsible for compliance with this policy. Failure to do so may result in disciplinary action. Where appropriate this may be considered gross misconduct.

Liz Hillary has been appointed as the lead within the company for ensuring all aspects of data compliance and GDPR and should be the first point of contact for any concerns or queries anyone in the organisation has in respect to processing personal data.

Specific responsibilities for data lead:

- Developing and ensuring compliance with data protection policies and procedures
- Making staff and others aware of their responsibilities in respect of data protection
- Being a point of contact for staff and others about any data queries
- Being the point of contact for the ICO
- Undertaking any work in respect of subject access requests and any other queries from data subjects
- Monitoring compliance with Data protection policy and procedure
- Dealing with any breach issue and maintaining a record of any incidents

The Malthouse, Standish, Stonehouse
Gloucestershire GL10 3DL
T. 01453 822584

GDPR

The GDPR is designed to protect individuals and their personal data which is held and processed about them. It also gives them rights over the data that is processed.

There are some key definitions and themes that are of significance for everyone to understand.

DATA YOU CONTROL AND PROCESS

'*Controller'* means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

In simple terms - a person or business that uses data i.e. information that identifies someone such as a customer and decides the way in which that data is used (also known as "processed").

In reality this means any business. The business is the data controller and employees act on behalf of the business (however they are not data controllers or processors in their own right).

'*Processor'* means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

'*Processing'* means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

In simple terms, this is everything that can be done with information e.g. storing it on a hard drive or server or keeping paper records (in a filing system i.e. in any way that is structured e.g. client files or HR files).

'Personal Data' is information relating to an identified or identifiable natural person ('data subject' or person). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, e.g. a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

In simple terms this means any information that identifies a living person.

This is a comprehensive (but not exhaustive) list of what ordinary data any business might typically hold and the groups a business might hold it under, e.g. membership list:

- Contact details of customers, clients, employees, contractors: Name, address, telephone number(s), email address, emails, IP address, bank details, notes kept of meetings, HR/ employee records, photos, CCTV, ID cards, financial information, membership lists, subscriber lists.

The Malthouse, Standish, Stonehouse
Gloucestershire GL10 3DL
T. 01453 822584

Special Category Data is information which you might previously have thought of as sensitive information. Article 9 of GDPR defines this information as:

> "Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited".

Data Protection Principles

The GDPR is based around a set of principles which are the starting point to ensure compliance with the Regulation. Everybody working in, for and with JPR Environmental must adhere to these principles in performing their day-to-day duties.

The principles require JPR Environmental to ensure that all personal data and special category data is:

1. Processed lawfully, fairly and in a transparent manner in relation to the subject ('lawfulness, fairness and transparency')

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which personal data are processed ('storage limitation')

6. Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures ('integrity and confidentiality')

Fairness and Lawfulness

The purpose of GDPR and UK data protection laws is not to prevent the processing of data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is in this case JPR Environmental, and who the data controller's representative is, in this case Liz Hillary and, the purpose for which the data is to be processed, retention periods and the legal basis for doing so, and the identities of anyone to whom the data may be disclosed or transferred.

The Malthouse, Standish, Stonehouse
Gloucestershire GL10 3DL
T. 01453 822584

GDPR allows processing of data for specific purposes, which are where it is needed:

- for the performance of a contract, such as an employment contract
- to comply with a legal obligation
- in order to pursue our legitimate interests (or those of a third party) and where the interests and fundamental rights of the data subject do not override those interests
- to protect the data subject's vital interests
- in the public interest, or
- in situations where the data subject has given explicit consent.

We, as data controller, will only process data on the basis of one or more of the lawful bases set out above. Where consent is required, it is only effective if freely given, specific, informed and unambiguous. The data subject must be able to withdraw consent easily at any time and any withdrawal will be promptly honoured.

Special categories of data and criminal convictions data will only be processed with explicit consent of the data subject, unless the data controller can rely on one or more of the other lawful bases set out above, and any additional legal bases for processing specific to these types of data. JPR Environmental also processes this type of data for reasons related to employment of staff.

Transparency

We will provide all required, detailed and specific information to data subjects about the use of their data through appropriate Privacy Notices which will be concise, transparent, intelligible, easily accessible and in clear and plain language.

Purpose Limitation

Data may only be processed for the specific purposes notified to the data subject via the Privacy Notice. This means that data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose via a new or amended Privacy Notice before any processing occurs.

Data Minimisation

Data should only be collected to the extent that it is required for the specific purposes notified to the data subject in the Privacy Notice. Any data which is not necessary for those purposes should not be collected in the first place.

Accuracy

Data must be accurate, complete and kept up-to-date. Steps should therefore be taken to check the accuracy of any data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be amended or destroyed.

The Malthouse, Standish, Stonehouse
Gloucestershire GL10 3DL
T. 01453 822584

Storage Limitation

Data should not be kept longer than is necessary to carry out the specified purposes. This means that data should be destroyed or erased from our systems when it is no longer required.

Security, Integrity and Confidentiality

We will ensure that appropriate technical and organisational security measures are taken against unlawful or unauthorised processing of data, and against the accidental loss of, or damage to, data. Data subjects may contact the Office of the Information Commissioner or apply to the courts for compensation if they have suffered damage from such a loss.

We will put in place procedural and technological safeguards appropriate to our size, scope and business, our available resources and the amount of data we hold, to maintain the security of all data from the point of collection to the point of destruction.

We will consider and use, where appropriate, the safeguards of encryption, anonymisation and pseudonymisation (replacing identifying information with artificial information so that the data subject cannot be identified without the use of additional information which is kept separately and secure).

Any documentation retained in paper form or kept in our offices is located in locked cabinets and/or in secure offices (with appropriate access control) which are both alarmed and monitored.

We will regularly evaluate and test the effectiveness of these safeguards. Employees have a responsibility to comply with any safeguards we put in place.

Maintaining data security also means guaranteeing the confidentiality, integrity and availability of the data, defined as follows:

- *Confidentiality* in respect of internal systems, means that only people who are authorised to use the Data can access it.
- *Integrity* means that Data should be accurate and suitable for the purpose for which it is processed.
- *Availability* means that authorised users should be able to access the Data if they need it for authorised purposes.

If you have access to personal information, you must:

a) only access the personal information that you have authority to access, and only for authorised purposes;
b) only allow other JPR Environmental staff to access personal information if they have appropriate authorisation;
c) only allow individuals who are not JPR Environmental staff to access personal information if you have specific authority to do so from Liz Hillary;
d) keep personal information secure;
e) not remove personal information, or devices containing personal information (or which can be used to access it), from JPR Environmental 's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device.

You should contact Liz Hillary if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

a) processing of personal data without a lawful basis for its processing or data or sensitive (special category) data,
b) any data breach
c) access to personal information without the proper authorisation;
d) personal information not kept or deleted securely;
e) removal of personal information, or devices containing personal information (or which can be used to access it), from the Company's premises without appropriate security measures being in place;
f) any other breach of this policy or of any of the data protection principles set out above.

Transfer Limitation

We will not transfer Data to any recipients outside the European Economic Area (EEA). That said, and from time to time we may pass personal data such as your name and email address to other services that we use to send out communications (both electronic and print). However, your personal data will remain in the EU or countries considered by the EU to have equivalent policies such as Jersey, Guernsey, Switzerland, New Zealand and Canada. Companies based in the USA that have certified with the EU-US Privacy Shield programme are also considered to be permitted destinations by the EU (this includes popular US products like Microsoft Office 365, DropBox and MailChimp).

Failure to follow rules on data security may be dealt with via the disciplinary procedure.

Rights of the data subject

The GDPR gives rights to individuals in respect of the personal data that any organisations hold about them.

Everybody working for JPR Environmental must be familiar with these rights and adhere to JPR Environmental procedures to uphold these rights.

These rights include:

- Right of information and access to confirm details about the personal data that is being processed about them and to obtain a copy;
- Right to rectification of any inaccurate personal data;
- Right to erasure of personal data held about them (in certain circumstances);
- Right to restriction on the use of personal data held about them (in certain circumstances);
- Right to portability – right to receive data processed by automated means and have it transferred to another data controller;
- Right to object to the processing of their personal data;
- Right not to be subject to a decision based solely on automated processing (including profiling).

If anybody is aware of a request for information about them from a data subject, they must inform the lead in the organisation immediately as there is only one month to respond to these requests.

The Malthouse, Standish, Stonehouse
Gloucestershire GL10 3DL
T. 01453 822584

Breaches

A data protection breach is defined as “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”.

Everyone working for and with JPR Environmental has a duty to report any breach or suspected breach without delay to the data lead who will determine what steps to take. It may be that the ICO or the data subjects who’s data has been breached need to be informed. If so, this must be done within 72 hours of anyone in the company becoming aware of the breach or suspected breach.

The data lead will also keep a record of each and all breaches and suspected breaches.

Confidentiality and data sharing

JPR Environmental must ensure that they only share personal information with other individuals or organisations where they are permitted to do so in accordance with data protection law.

Wherever possible you should ensure that you have the data subject’s consent before sharing their personal data, although, it is accepted that this will not be possible in all circumstances, for example if the disclosure is required by law.

Any further questions around data sharing should be directed to the lead for data protection.

Data Protection Impact Assessments (DPIAs)

Where processing is likely to result in a high risk to an individual’s data protection rights (eg where JPR Environmental is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

a. whether the processing is necessary and proportionate in relation to its purpose;
b. the risks to individuals; and
c. what measures can be put in place to address those risks and protect personal information.

Before any new form of technology is introduced, the manager responsible should therefore contact Liz Hillary in order that a DPIA can be carried out.

During the course of any DPIA, JPR Environmental will seek the advice of Liz Hillary and the views of employees and other relevant stakeholders.

Complaints

Complaints relating to breaches of the GDPR and/or complaints that an individual’s personal data is not being processed in line with the data protection principles should be referred to Liz Hillary without delay.

The Malthouse, Standish, Stonehouse
Gloucestershire GL10 3DL
T. 01453 822584

Other Related Policies

Breach policy and procedure
Subject Access Requests policy and procedure
Privacy notices

Training

JPR Environmental will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Consequences of failing to comply

It is important that everybody working for JPR Environmental understands the implications if the company fails to meet its data protection obligations.

Failure to comply with the policy:
- puts at risk the individuals whose personal information is being processed;
- carries the risk of significant civil and criminal sanctions for the individual and JPR Environmental; and
- may, in some circumstances, amount to a criminal offence by the individual.

It can also:
- lead to potentially irreparable reputational damage and adverse publicity for JPR Environmental
- Suspension/withdrawal of the right to process personal data by the ICO and imposition of different processing methods
- Loss of confidence in the integrity of the business's systems and procedures
- Fines and damages.

An employee's failure to comply with any requirement of this policy may lead to disciplinary action and could result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about anything in this policy, do not hesitate to contact Liz Hillary.

Last Reviewed: 07/02/2019

The Malthouse, Standish, Stonehouse
Gloucestershire GL10 3DL
T. 01453 822584

I have read and understood JPR Environmental's Data Protection Policy (which conforms to the Data Protection Act 2018) and agree to abide by its terms:

Name:	
Signature:	
Date:	
Name:	
Signature:	
Date:	
Name:	
Signature:	
Date:	
Name:	
Signature:	
Date:	
Name:	
Signature:	
Date:	
Name:	
Signature:	
Date:	
Name:	
Signature:	
Date:	
Name:	
Signature:	
Date:	
Name:	
Signature:	
Date:	