Document details:

Title	Data Protection Policy
Document ID	EXT006
Version number	1.03/0223
Status	Published
Published date (web)	02/23
Author	Board of Directors
Approved by	Board of Directors
Review date	02/24
Review frequency	Annual

Revisions:

Version	Date	Description	Revision
1.01	01/22	Original document	Original copy
1.02/0123	01/23	Updated	Review by Board of Directors
1.03/0123	09/23	Updated	Added page 1 document details

Data Protection Policy

Aim and scope of policy
The Company, GrillaTech ("we", "us", "they", "our") is committed to being transparent about how we collect and use the personal data of our workforce, and in the course of our business operations, in accordance with our data protection obligations and any relevant domestic laws or related policies.

This policy applies to the processing of personal data in manual and electronic records kept by the Company in connection with its human resources function as described below. It also covers the Company's response to any data breach and other rights under the General Data Protection Regulation.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

Questions about this policy should be addressed to tilly.dineen@grillatech.com using the Data Subject Rights request form (as per the Data Subject Rights Policy) where appropriate.

The Company as Controller
Where we are the data controller, data subjects will be provided with the reasons for the processing of their personal data, how we use such data and the legal basis for processing in its "privacy notices". It will not process personal data of individuals for other reasons.

Definitions

Personal Data	Information that relates to an identified or identifiable person (a "data subject"). An identifiable person is one who can be identified, directly or indirectly from an identifier, e.g. a person's name, identification number, location, online identifier. It can also include pseudonymised data.
Processing	Any use that is made of the data, or sets of personal data e.g., collecting, storing, amending, disclosing or destroying.
Special categories of personal data	Information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic/biometric data (where used for ID purposes).
Criminal offence data	Data which relates to an individual's criminal convictions and offences.
Data Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means (including 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).

Where third parties process data on behalf of the Company, such parties do so under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures in order to maintain the Company's commitment to protecting data.

Types of data held
Relevant individuals should refer to the Company's privacy notices and Retention Policy for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

Data protection principles
All personal data obtained and held by the Company will be processed in accordance with the data protection policies.

Principle	**The Company;**
Fair, Lawful and Transparent	Processes personal data lawfully, fairly and in a transparent manner in relation to the data subject.
Purpose Limitation	Collects personal data only for specified, explicit and legitimate purposes and is not further processed in a manner which is not compatible with this.
Data Minimisation	Processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
Accuracy	Keeps accurate personal data only for the period necessary for processing.
Storage Limitation	Adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing and accidental loss, destruction or damage.
Security	Data is processed in a manner which ensures its security.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed;
- the right of access;
- the right for any inaccuracies to be corrected (rectification);
- the right to have information deleted (erasure);
- the right to restrict the processing of the data;
- the right to portability;
- the right to object to the inclusion of any information;
- the right to regulate any automated decision-making and profiling of personal data.

Further details are outlined in the Data Subject Rights Policy.

Impact assessments
Where processing may result in risks to privacy, the organisation will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for

individuals and the measures that can be put in place to mitigate those risks, and overviewing the effectiveness and integrity of all of the data which must be protected.

Access to data
Relevant individuals have a right to be informed whether the Company processes personal data relating to them and to access the data that the Company holds about them. Further information can be found in the Data Subject Rights Policy (including Subject Rights Access form).

Data disclosures
The Company may be required to disclose certain data/information to any person but will only do so when strictly necessary for the purpose. The circumstances leading to such disclosures include:

- any employee benefits operated by third parties;
- disabled individuals - whether any reasonable adjustments are required to assist them at work;
- individuals' health data - to comply with health and safety or occupational health obligations towards the employee;
- for Statutory Sick Pay purposes;
- HR management and administration - to consider how an individual's health affects his or her ability to do their job;
- the smooth operation of any employee insurance policies or pension plans.

Data security
The Company adopts procedures designed to maintain the security of data when it is stored and transported. More information can be found in the Data Transfer Security Policy.

In addition, employees must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them;
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people;
- check regularly on the accuracy of data being entered into computers;
- always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them;
- use computer screen blanking to ensure that personal data is not left on screen when not in use.
- comply with any other relevant IT policies relating to data security.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by Managing Director**.** Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary;

- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted;
- ensuring that laptops or USB drives are not left lying around where they can be stolen.

This also applies to the use of external social networks, used increasingly for business activities. Whilst the internet has many advantages, it could expose the Company to greater reputational risks, either through ignorance or malicious intent. There is a risk that confidential and proprietary information could be compromised. Employees are personally responsible for their social media and online communications. The right to monitor Company systems is outlined in the IT Systems Use Policy under Monitoring.

Failure to follow the Company's rules on data security, including any significant or deliberate breaches of the policy may be dealt with via the Company's disciplinary procedure and may constitute gross misconduct which could ultimately lead to dismissal without notice.

International data transfers
The Company does not transfer personal data to any recipients outside of the EEA.

Breach notification
A data breach is a breach of security leading to the accidental or unlawful destruction, loss, unauthorised disclosure of, or access to, personal data transmitted, stored or processed, whether held in electronic form, physical records, and regardless of what media it is stored on. For these purposes, a breach is identifiable as a security incident which has affected the confidentiality, integrity or availability of personal data.

Examples of a data breach may include;
- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a data controller or data processer
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

In cases where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the Company becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual. A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation. The Company will consider the type of breach, the type of data involved (including special characteristics), the nature and volume of personal data, the ease of identification of individuals, sensitivity of consequences for the individuals involves and the resultant severity of the breach considering the nature of the business.

If the breach is sufficient to warrant notification to the public, the Company will do so without undue delay.

Accountability
Data subjects are responsible for helping the Company keep their personal data up to date and should let the Company know if data provided has changed (e.g. change of address/bank details).

Only those personnel who require access to, and use of, personal data in order to fulfil the requirements of their roles will be permitted access to data held by the Company. Where this is the case, the Company relies on individuals to help meet its data protection obligations under the policy and legislation.

Individuals who have access to data are required to;

- Be made fully aware of both their individual responsibilities and those of the Company in accordance with the Data Breach Policy and applicable law;
- Access only data that they have authority to access and only for authorised purposes;
- Not disclose data except to individuals (whether inside or outside of the Company) who have appropriate authorisation;
- To keep data secure
- Not to remove personal data, or devices containing data or that can be used to access data, from the Company's premises without adopting appropriate security measures (e.g. encryption or password protection) to secure data and the device;
- Not to store personal data on local drives or on personal devices that are used for work purposes;
- Comply with any requirements of related IT and data protection policies.
- To report data breaches/potential breaches as per the Data Breach Policy as soon as made aware to Tilly Dineen (tilly.dineen@grillatech.com)

Training
All employees are responsible for their compliance and awareness with upholding the Data Protection obligations of the Company and the relevance to processing any data within their role. Employees who are responsible for ensuring data security should understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Company's policies and procedures.

Data protection compliance
***[Insert name]* Tilly Dineen is the Company's appointed compliance officer in respect of its data protection activities. She can be contacted at:**
T: 0333 7722 127
E: tilly.dineen@grillatech.com
E: admin@grillatech.com