Date Protection Policy

Version	1.1
Reference Number	EGDP1
Date in Use From	26/02/2024
Last Reviewed	26/02/2024
Written By	HR & ESG Manager (KFM)
Approved By	HR & ESG Manager (KFM)
Process Owner	HR & ESG Manager (KFM)
Security Marking	Official

Contents

Introduction

This policy sets out the Easby Group responsibilities and accountability regarding data protection in line with the Data Protection Act 2018 (DPA) and UK General Data Protection Regulations (GDPR) and applies to all those working for a Group company.

Compliance with GDPR is overseen by the Information Commissioners Officer (ICO), and where required individual Easby Group companies will register with the ICO.

For Easby Group to conduct its business in line with data protection laws and regulations including GDPR it expects that all Easby Group staff comply with this policy, and training is provided to support everyone in understanding their responsibilities.

The Group process two types of personal data; staff data and data in relation to customers and suppliers which may include personal data for those who are representing their organisation when dealing with the Group, for example a person signing a contract.

Data Protection is a serious matter and any breach of this policy or related documents may result in disciplinary action for Easby Group employees.

Scope

As a data controller, this policy covers all personal data that Easby Group stores and processes about our clients, perspective clients, suppliers and employees.

Objectives

Easby Group will:

- Adhere to the GDPR Principles for controlling personal data.
- Respect and support individuals' rights concerning their personal data, as detailed in GDPR.
- Ensure data protection is built in by design and default to all processes that include personal data.
- Undertake a data protection impact assessment for processes that have a high risk of a data breach which includes personal data.
- Consider and implement organisational and technology measures to mitigate risks to personal data.
- Should Easby Group transfer personal data to a third party located in a country outside of the EEA, consider their compliance with an approved transfer mechanism such as the EU-US Privacy Shield.
- Report data breaches in line with ICO requirements.
- Handle complaints according to the Easby Group Complaints Process.
- Monitor and maintain records to support the accountability requirement of GDPR.
- Review and audit this Policy and supporting processes and procedures annually as a minimum.
- Correct any identified deficiencies in this Policy and the supporting processes and procedures within a defined and reasonable time frame.

Responsibilities

All employees and contractors of Easby Group have a responsibility for ensuring that personal data is collected, stored and handled appropriately.

To ensure the understanding of responsibilities when handling personal data, Easby Group will:

- Provide training to all employees on their responsibilities including security measures.
- Ensure that all existing customers, contractors and sub-contractors are aware of, and will adhere to this Policy and associated documentation.
- Include GDPR readiness status as part of the selection process of new associates, sub-contractors and other third parties used as Data Processors.

Data Protection Principles

There are six data protection principles detailed in Article 5 of the GDPR. This section outlines the responsibilities arising from these principles and the Easby Group approach for each.

1. Lawful, Fair and Transparent Data Processing

The requirement of this principle is that personal data must be processed lawfully, fairly and in a transparent manner in relation to individuals.

Easby Group maintains a register of all personal data that it stores and processes, the purpose, the lawful bases for doing so, and any personal data that is shared with third parties.

This information is communicated with Data Subjects via The Easby Group Privacy Notice (such as the one on the Easby Groups website) or within terms and conditions or other contracts.

In all instances these will be written in concise, understandable language which is appropriate for the audience.

The relevant Privacy Notice, or link to Privacy Notice, will be provided at the point of collection of personal data, or as soon as its practicably possible.

2. Purpose Limitation

Under this principle personal data can only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. *(NB: Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes)*.

Easby Group 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, Easby Group is committed to seeking such consent.

If Easby Group would like to use personal data for any reason apart from what was originally agreed under the first principle (see above), we will seek explicit consent for the new reason(s).

Consent maybe withdrawn by an individual at any time. The mechanism by which this can be done will be detailed in at least the Easby Group Privacy Notice(s).

3. Data Minimisation

The requirement of this principle is that any personal data which is stored and processed should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Easby Group will identify for each Data Subject the purpose of the processing and the minimum personal data it requires for the purpose. This is further detailed in the Easby Group Records Management Policy.

4. Accuracy of Data

Easby Group will take all reasonable steps to ensure data is accurate and will periodically check the accuracy of any personal data it stores and processes. Where reasonable any amendments required which are identified or notified by an individual will be made as soon as is practicable

5. Storage Limitation

The requirement of this principle is that personal data is 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.
Easby Group identify the retention period(s) for personal data stored and personal data is deleted as soon as is practicable after that time.
(NB: personal data may be stored for longer periods insofar as the personal data will be

processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals).

6. Integrity, confidentiality and security

Under this requirement personal data is processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using relevant technical or organisational measures.

Easby Group uses appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data. Easby Group retains personal data only for the required legal, trading, or contractual period, and thereafter personal data is electronically deleted and any hard copy documentation securely shredded.

Rights of Individuals

GDPR provides eight rights for individuals, and this section summarises each of these and provides the Easby Group process associated with each.

Where Easby Group is deemed to be a Data Processor we will engage with the Data Controller(s) on how requests from individuals will be fulfilled.

When an individual makes a request regarding any of these rights, before any action is taken concerning the request, Easby Group will check that:

- The request is reasonable,
- Their identity is confirmed,
- There is no impact on other individuals' personal data and their rights, and,
- There is no legal, regulatory or contractual requirement to retain the data in its current form.

Right to be informed

The Right to be informed encompasses Easby Group's obligations to provide 'fair processing information' to data subjects, typically through a Privacy Notice, and emphasises the need for transparency about how personal data is used.

Easby publish privacy notices for customers on our websites, and the privacy notice for staff is published on our HR system, and embedded into the Employee Handbook, which is issued to all new starters before their first day.

Right of Access

Individuals have the right to access and receive a copy of their personal data and supplementary information by submitting a subject access request. Details of how and who to submit a subject access request to are contained in the privacy notices.

Right to Rectification

The GDPR gives individuals the right to have their personal data rectified where it is inaccurate or incomplete. Details of who to contact to exercise this right are provided in the Easby Group Privacy Notice.

Where a request is received once the checks detailed at the top of this section are complete, Easby Group will amend the relevant data as soon as is reasonably possible. An email will be sent to the requesting individual to confirm and act as a record of the completion of the request.

Right to Erasure

The Right to Erasure is also known as 'the right to be forgotten', and the broad principle underpinning this right is that an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Where a request is received once the checks detailed at the top of this section are complete, Easby Group will delete the relevant data as soon as is reasonably possible. An email will be sent to the requesting individual to confirm and act as a record of the completion of the request.

Right to Restrict Processing

Individuals have a right to 'block' or suppress processing of their personal data in certain circumstances. Where processing is restricted, Easby Group is permitted to store the personal data, but not further process it, and can retain sufficient information about the individual to ensure that the restriction is respected in future.

After completing the checks detailed at the top of this section, Easby Group will not process the requesting individual's personal data until notified. An email will be sent to the requesting individual to confirm and act as a record of this.

Right to Data Portability

The Right to Data Portability allows individuals to obtain and reuse their personal data for their own purposes. It allows them to move, copy or transfer their personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

This right only applies to data the individual has provided to the data controller directly. Whilst this right applies to Easby Group it is unlikely, give the nature of the data held, that any data held would be of benefit to transfer.

Right to Object

Individuals have the right to object to:

- Direct marketing (including profiling)
- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling).
- Processing for purposes of scientific/historical research and statistics.

Details of who to contact to exercise this right and how to complain are provided in the Easby Group Privacy Notice.

Rights related to Automated Decision-Making including Profiling

Companies can only carry out this type of decision-making where the decision is:

- Necessary for the entry into or performance of a contract,
- Authorised by applicable law, or
- Based on the individual's explicit consent.

No automated decision making (nor profiling) is undertaken by Easby Group either directly or on behalf of third parties. Should it ever be, then a process will be put in place and this Policy document updated.

Appendix 1 – Definitions

Requirement	Definition
Personal Data	Any information relating to an identified or identifiable person where that person can be identified, directly or indirectly, by reference to an identifier such as a name or to one or more factors specific to the physical, genetic, mental, economic, cultural or social identify of that person
Special Categories of Personal Data	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 person, data concerning health or data concerning a person's sex life or sexual orientation.
Child	The GDPR defines a child as anyone under the age of 16 years old. This may be lowered to 13 by Member State Law as within the UK. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained.
Data Protection Impact Assessments	An assessment undertaken prior to the processing of the impact of the envisaged processing operations, where such processing uses new technology and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of persons, on the protection of personal data.
Data Controller	Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing personal data.
Data Processor	Natural or legal person, public authority, agency or body which processes personal data on behalf of the Data Controller.
Third Party	A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal 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, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Filing Systems	Any structured set of personal data which are accessible according to the specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, agrees to the processing of personal data relating to him or her.
Data Subject	An identified or identifiable natural (living) person
Profiling (Automated Processing)	This is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, or measures based on profiling and the envisaged effects of profiling on the individual.

Personal 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.
Supervisory Authority	An independent public authority which is established by the UK responsible for monitoring the application of the Regulation. Within the UK this is the Information Commissioner's Office.
Information Notice or Privacy Notice	A notice given to the data subject, in writing or other means including orally and by electronic means, which sets out in a concise, transparent and intelligible and easily accessible way using clear and plain language the following information: • Identity and contact details of the controller. • Purposes of processing and legal basis for processing. • Recipients or categories of recipients of the personal data. • Details of data transfers outside the EU, including how the data will be protected. • The retention period for the data, or if not possible to give, the criteria used to set this. • That the person has the right to access and port data, to rectify, erase and restrict his or her personal data, to object to processing and if processing is based on consent, to withdraw consent. • That the person can complain to the supervisory authority. • Whether there is a legal or contractual requirement to provide the data and the consequences of not providing the data. • If there will by any automated decision taking including information about the logic involve and the significance and consequences of the processing for the person.
Encryption	The process of encoding personal data in such a way that only authorised parties can access it.
Breach register	A register documenting any personal data breaches, comprising the facts relating to the breach, its effects and the remedial action taken.
Template letters	Letters containing standard wording to be used with additional wording added specific to the information being provided in the letter.
Access request Timescale	Information must be provided without delay and at the latest within one month of receipt.

Appendix 2 – Version Control

Date	Version	Notes on amendments	Updated by
Mar-22	1	Re-branded Easby Policy based on earlier Rebound Policy	KFM
01/03/24	1.1	Updated to include all Group companies with minor rewording / formatting changes to aid clarity.	KFM