Newable

# Data Protection Policy

## Version 1.0

April 2021

Newable

# Version Control

| Version | Owner | Reviewer | Changes | Approval date | Next Review |
|---|---|---|---|---|---|
| 1.0 | Joanne Wilkinson | Michael Walsh | Initial version or first version uploaded on portal - see ESG share for historical information | 04/2021 | 03/2022 |

# Background

The General Data Protection Regulation (GDPR) entered into force across the EU on 25th May 2018, replacing the EU Data Protection Act (DPA). GDPR introduced new elements and significant enhancements, such as new transparency and individuals' rights provisions. The GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. The Company must document what personal data it holds, where it came from and who it may be shared with, as well as how long it will be held.

There are also changes to consent which must be explicit, non-ambiguous and given freely, and consent can be withdrawn.

Information processed by the Company about its employees, other workers, clients and suppliers must be collected and used fairly, stored safely and not disclosed unlawfully. The Company may need to disclose employees' personal data to third parties from time to time, including governmental and quasi-governmental bodies for social security and other purposes, future employers for providing references and other information, and to future purchasers of the Company or business in which you work.

This policy describes the Company's arrangements for protecting the personal data it holds. The Company and all its employees who process or use personal information must ensure that these principles are followed at all times.

Newable

# Policy

## Processing and personal data

**Processing** includes collection, holding, retention, destruction and use of personal data.

**Personal data** is defined as information relating to an identifiable living individual, from which the individual's information can be readily extracted, held in any format, including electronic (i.e. websites and emails), paper-based and photographic.

Personal data may include information of a sensitive personal nature including information concerning employees':

- racial or ethnic origins
- religious beliefs or other beliefs of a similar nature (for example, if particular religious holidays are taken as paid holiday)
- membership or non-membership of a Trade Union
- physical or mental health or condition
- commission or alleged commission of any offence
- sexual life or sexual orientation
- biometric or genetic data

This is not an exhaustive list.

## Data protection principles

The data protection principles set out the main responsibilities for organisations and require that personal data should be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and is not further processed in any manner incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
- kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data is processed; and
- 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 is responsible for, and must demonstrate, compliance with the principles.

The GDPR places more emphasis on being accountable for and transparent about the lawful basis for processing information.

## Lawful basis for processing

You must have a valid lawful basis for processing personal data and there are six available lawful bases for processing (consent, contract, legal obligation, vital interests, public task and legitimate interests). Most lawful bases require that processing is “necessary”. You must determine your lawful basis before you begin processing, and you should document it. The Company’s privacy notice includes the lawful basis for processing. The GDPR places more emphasis on being accountable for and transparent about your lawful basis for processing. An individual always has the right to object to processing for the purposes of direct marketing, whatever lawful basis applies.

At least one of the following lawful bases for processing must apply whenever you process personal data:

a. **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
b. **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
c. **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
d. **Vital interests:** the processing is necessary to protect someone’s life.
e. **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
f. **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests.

Many of the lawful bases for processing depend on the processing being “necessary”. This does not mean that processing always has to be essential. However, it must be a targeted and proportionate way of achieving the purpose. You need to keep a record of which basis you are relying on for each processing purpose, and a justification for why you believe it applies.

## Responsibilities of employees

You are expected to maintain confidentiality in your work where appropriate but you

should also review your own procedures for handling personal data.

As an employee you are responsible for:

a. checking that any information that you provide to the Company in connection with your employment is accurate and up to date; and
b. informing the Company of any changes to information that you have provided, e.g. change of address, either at the time of employment or subsequently. The Company cannot be held responsible for any errors unless you have provided the information.

If as part of your responsibilities you collect information at work about other individuals, you must comply with the guidelines for employees as set out in the Code of Practice.

## Code of practice

**Data security**

You are responsible for ensuring that:

- any personal data that you hold is kept securely; and
- personal information is not disclosed either orally or in writing or via web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Unauthorised disclosure will be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should:

- be kept in a locked filing cabinet, drawer, or safe; or
- if it is computerised, be coded, encrypted or password-protected on a drive that is regularly backed up; and
- if a copy is kept on a disk or other removable storage medium, that medium must itself be kept in a locked filing cabinet, drawer or safe.

**Subject consent**

In many cases, the Company can only process personal data with your consent. In some cases, if the data is sensitive explicit consent must be obtained.

The Company may ask for information about particular health needs, such as allergiesto particular forms of medication, or any medical condition such as asthma or diabetes. The Company will only use this information in the protection of your health and safety, but will need consent to process this data, for example in the event of a medical emergency.

**Processing sensitive information**

Sometimes it is necessary to process certain sensitive information, for example about criminal convictions or health. This may be necessary to ensure that the Company is a safe place of work for everyone, and also for the Company to operate other policies. In some cases (for example where criminal convictions are concerned) an offer of employment may be conditional on the employee's permission for such data to be processed. In all such cases, as this information is considered sensitive, employees will be asked to give their explicit consent for the Company to process this data.

**Retention of data**

The Company has a duty to retain some employee personal data for a period of time after their departure from the business. This is for legal reasons and for other purposes such as being able to provide references or issues relating to pensions and taxation. Different categories of data will be retained for different periods of time, in accordance with the firm's record retention policy.

**Transfer of data outside the EEA**

It may be necessary to transfer personal data outside of the European Economic Area in order that the Company may properly carry out its duties, rights and obligations as your employer, primarily for personnel, administrative and pay roll purposes. As far as possible, you will be notified when such a transfer has taken place and for what purpose. The Company will also comply with a reasonable request by the employee to reveal the identity of the third party to whom the data has been disclosed.

**Secure storage, handling, use, retention and disposal of Criminal Records Bureau (CRB) disclosures and disclosure information**

Some parts of the Group, such as HR, use the CRB disclosure service to help assess the suitability of applicants for positions of trust, such as finance positions. The Company complies with the CRB code of practice and other legislation regarding the correct handling, use, storage, retention and disposal of disclosures and disclosure information.

*Storage and access*

Disclosure information is kept securely in lockable, non-portable, storage containers

or secure IT systems, with access strictly controlled and limited to those who are entitled to see it as part of their duties.

*Handling*

Disclosure information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom disclosure information has been revealed and it is a criminal offence to pass this information to anyone who is not entitled to receive it.

*Usage*

Disclosure information is only used for the specific purpose for which it was requested and for which the subject's full consent has been given.

*Retention*

Once a decision has been made, we do not keep disclosure information for any longer than is necessary. This is generally for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints. If, in very exceptional circumstances, it is considered necessary to keep disclosure information for longer than six months, we will consult the CRB about this and will give full consideration to the data protection and human rights of the individual before doing so. Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will prevail.

*Disposal*

Once the retention period has elapsed, we will ensure that any disclosure information is immediately destroyed by secure means, i.e. by shredding, pulping or burning or permanent deletion of information on IT systems. While awaiting destruction, disclosure information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack). After disposal we will not keep any photocopy or other image of the disclosure or any copy or representation of the contents of a disclosure. However, notwithstanding the above, we may keep a record of the date of issue of a disclosure, the name of the subject, the type of disclosure requested, the position for which the disclosure was requested, the unique reference number of the disclosure, and the details of the decision taken.

Should at any time disclosure documents containing personal information be lost we will immediately report this to the Company's CRB-registered umbrella body, who will report the matter to the CRB.

# Your rights

## Right to access

All employees and other users are entitled to:

- know the information that the Company holds and processes about them and why;
- know how to gain access to it;
- know how to keep it up-to-date and to rectify any errors; and
- know that the Company is working to comply with its obligations.

All employees and other users have a right to access certain personal data being kept about them either on a computer or in certain files.  Any person who wishes to exercise this right should make a request in writing, via a Subject Access Request (SAR), to the Data Protection Officer (DPO) or the Head of HR.

The Company must provide a copy of the information requested free of charge. However, the Company reserves the right to make an administrative charge for repeated, voluminous or vexatious requests for information.

The Company aims to comply with requests for access to personal information as quickly as possible, but will in any case ensure that access is provided within the statutory one month.

## Right to erasure

In the event that an employee believes that the Company is holding incorrect data or that the data has been held longer than is necessary, then the employee has the right to request erasure of the data. The request should be submitted to the DPO or Head of HR

## Right to rectification

In the event that an employee believes that the Company is holding inaccurate personal data, then a request can be submitted to the DPO or Head of HR to have the personal data rectified, or completed if it is incomplete. The Company will confirm to the employee that the inaccurate personal data has been rectified or completed if it is inaccurate.

Newable

# Reporting data protection incidents or breaches

The Company is responsible for protecting the information it holds and is legally required under the GDPR to ensure the security and confidentiality of personal information processed. Employees must take care to protect information and to avoid a security incident or breach, especially where the result is a data breach when personal information is lost or disclosed inappropriately to an unauthorised person. All data incidents or breaches should be reported immediately to the DPO. The GDPR introduces a mandatory requirement to report certain types of personal data breaches, which are likely to result in risk to the rights and freedoms of individuals to the Information Commissioner's Office (ICO).

A data breach is defined as a:

- Confidentiality breach – an unauthorised or accidental disclosure of or access to personal data;
- Integrity breach – unauthorised or accidental alteration
- Availability breach – accidental or unauthorised loss of access to or destruction of data (for example, by a power cut or systems failure)

The DPO is responsible for reporting any material breaches to the ICO no later than 72 hours after having become aware of the breach. Where the notification to the ICO is not made within 72 hours, it should be accompanied by reasons for the delay. If there is a high risk to individuals, then they must be informed of the material data breach as well.

The ICO has the power to impose fines of up to 4% of total annual turnover or Euro 20,000,000 for material data breaches.

Newable

# Privacy Impact Assessments

Privacy Impact Assessments (PIAs) are a tool to help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective PIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. An effective PIA will be used throughout the development and implementation of a project, and examples of when a PIA should be undertaken include installing new IT systems, pooling sets of personal data with other organisations, and using existing data for a new and unexpected or more intrusive purpose.