1st Floor, Beech House, Millenium Park, Osbertown, Naas, Co Kildare, Ireland.

DATA RETENTION POLICY

Purpose

This document sets out the data retention guidelines for retaining different types of personal data within our company. The policy applies to all 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.

Policy Statement

The retention of data by our company varies from piece of data to piece of data. It is our objective that data is deleted as quickly as possible once the purpose for which it was collected has been served and expired.

However, the company must comply with various statutory responsibilities and obligations and therefore immediate deletion is not always achievable. 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

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

Source of Obligation	Retention Period
Revenue Commissioners, Collector General, Companies Acts legislative provisions	6 years rolling retention of records
Personal Injuries related records	Records are retained for a period of 3 years past the date of the cause of action, unless it involves a minor, in which case the retention period will be up until 3 years after the minor reaches the age of 18.

Breach of Contract related records	Records are retained 6 years from the date of the breach
Membership Application Forms	Membership Application Forms are retained for the duration of their membership and for 12 months after the membership has finished or completed.
Employment contract/terms of employment related information	Duration of the employment – this includes everything from the application form, interview notes, contract related, performance appraisals, references, the retention period will be the duration of employment.
Disciplinary/Grievance Documentation	Retained for the duration of the employment of the relevant parties
Organisation of Working Time – time sheets/holiday and public holiday records National Minimum Wages Protection of Employment – Temporary Agency Workers, Part Time Workers, Fixed Term Workers Protection of Young Persons	3 years post the termination of the employment. Records kept are sufficient to show compliance with legal obligations in accordance with the statutory provisions.
Parental Leave Related	8 years – records kept show the dates when a qualifying employee availed of the parental leave and force majeure leave provisions
Employment Equality	All records of interviews and applications are kept for a period of one year post the application period in order to exhaust the statute of limitations in relation to a potential claim
Health and Safety Records	All records relating to health and safety will be kept for a period of 10 years
Data Law Compliance	Records in relation to our compliance with Data Law and GDPR will be kept for a five year period.

Retention of encrypted data

Any information retained under this policy is stored in an encrypted format. Encryption keys are retained as long as the data that the keys decrypt is retained.

Data duplication

We will endeavour to ensure that there is no duplication of data. In this regard, once data subject information is received by email, that information will be uploaded onto our Administration Management System/Membership Database and the originating email is deleted, this is supported in relevant Standard Operating Procedures.

Data Destruction

When the retention timeframe expires, we will actively destroy the data covered by this policy. Exceptions will only be made where there is a written application which has been given consideration by the company Data Protection Officer. Destruction will be verified by our IT contractors where it is soft copy information and certified by our shredding company where it is hard copy information. A database of deleted data subjects is kept which will contain only the bare minimum of data in order to verify the identification of that individual and that date of destruction will be kept to enable confirmation in the event of a Data Subject Access Request.

Responsibilities

Compliance, monitoring and review

The Data Protection Office has the overall responsibility for ensuring compliance with the requirements of the related legislation. All staff that deal with personal data are responsible for processing this data in full compliance with our relevant policies and procedures.

Reporting in case of a data breach

Data will only be accessed in our company by a relevant individual. A person becomes a relevant individual by virtue of employment or their volunteer role. In the case of possible data breach, the relevant individual who first identifies the breach or incident, must immediately report all details of the incident to the Data Protection Officer.

The Data Protection Officer is required to report a personal data breach to the competent Data Protection Authority, the Irish Data Protection Commissioner, not later than 72 hours after becoming aware of it. The notification must be made in accordance with the online questioning by the DPC that provides for details including:

- 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 Officer or in the alternative a contact point;
- the likely consequences of the data breach; and
- measures taken or proposed to address the breach and/or mitigate its effects.

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 Officer (DPO) must communicate the breach to the data subject(s) without undue delay. Such risk will be determined by the DPO. 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 Officer or in the alternative a 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

Staff must maintain all records relevant to administering this policy and procedure in electronic form in the company Administration Management System.

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

Terms And Definitions Relevant to this Policy:

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 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

Processing: any operation performed on personal data, whether or not 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