

Data Protection Policy

The Company is firmly committed to ensuring personal privacy and compliance with the Data Protection Acts 1988-2018 and the General Data Protection Regulation (GDPR) (together “the legislation”) and best practice guidelines and procedures in relation to all aspects of Data Protection.

All staff are required to comply with the legislation and assist the Company in complying with the legislation. Staff should protect the privacy and confidentiality of the personal data of customers, suppliers or employees. When dealing with personal data employees must employ the six core principles of Data Protection.

- 1. Personal Data must be obtained and processed fairly, legally and transparently.** The Company will obtain and process personal data fairly and in accordance with statutory and other legal obligation.
- 2. Personal Data can only be obtained for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.** The Company will only keep personal data for purposes that are specific, lawful and clearly stated.
- 3. Personal Data obtained must be adequate, relevant and limited to what is necessary in relation to the purpose for which it was obtained.**
- 4. Personal Data must be kept accurate and up to date.**
- 5. Personal Data must be kept only for so long as is necessary for the purpose for which it was obtained.**
- 6. Personal Data must be processed in a way that ensures appropriate security including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage, using appropriate technical and organizational measures.**

Definitions

Personal Data is “any information relating to an identified or identifiable living person” and includes names, addresses, PPS number, date of birth etc. Special Category Personal Data includes data relating to a person’s racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health information or sex life or sexual orientation.

Processing

As employer we process employee data on the following legal bases.

For example

- the performance of the employment contract (e.g., payment of salary);
- compliance with a legal obligation to which the employer is subject (e.g., deduction of taxes);
- to protect the vital interests of the employee (this is intended to cover urgent health or humanitarian situations e.g., sharing personal data with the police to help to protect the data subject); and
- to protect the legitimate interests of the employer (e.g., the transmission of personal data within a group of undertakings for internal administrative purposes).

It is important to note that the company have certain outsourced services such as accountancy etc. and so in order to comply with its legal obligations, the Company reserves the right to forward certain personal data for its employees to the relevant third parties. The company have taken extensive measures to ensure those third parties securely retain this information. Any information

forwarded may be processed by those parties. Information will be made available to the WRC / The Department of Social Welfare / Revenue should they request same.

Security

It is important to note that all data will be treated with the utmost confidentiality and the company will take security measures to ensure your personal data is not accessible to anybody other than those who are authorised to have access to the same.

Personal Data

In line with the requirements of the legislation, personal data should not be collected or retained if it is not needed and/or on the basis that it might be required in the future.

The types of information about individuals that the company collects will be reviewed periodically to ensure compliance with this requirement and in line with the company Data Protection Policy.

Each category of personal data will be assessed when determining retention periods as the company may have justifiable reason to retain certain types of personal data.

Data Breaches

In the circumstances of a certain or a potential data protection breach please notify the Managing Director immediately who will assess the breach to see if it is necessary to notify the Data Protection Commission. Staff are required to fully co-operate with all requirements of the Data Protection Commission, the Company and/or any other authorised person in the investigation of a breach.

Please note that failure to adhere to this policy may result in a disciplinary sanction, up to and including dismissal.

Data Retention Policy

The GDPR requirements ensure that personal data is not retained for longer than is necessary. We must be able to justify why we are retaining data and we must ensure that data retention is minimised.

In relation to employment documents, certain employment legislation prescribes a statutory minimum period to retain records which are outlined in the below table:

The table is enclosed within the Appendix of this Handbook for your information.

This table will be used as a guide but data can be retained longer than is outlined in the table if it can be justified.

Legislation	Data	Time Period
The Employment Equality Acts 1988 — 2008	• CVs • Interview Notes • Interview Assessment Forms • Offer Letters • Regrets	12 months from when the position was filled.
Organisation of Working Time Act 1997	• Records relating to weekly working hours • Holidays • PPS numbers	3 years (for both past and present employees). Responsibility of Payroll and may be extended for revenue requirements.

	• Statement of duties and the name and address of each employee.	
National Minimum Wage Act 2000	• Pay records, e.g., payslips showing compliance	3 years from the date of creation for both past and present employees. Responsibility of Payroll and may be extended for revenue requirements.
Terms of Employment (Information) Act 1994	• Terms and Conditions of Employment • Confidentiality Agreements • Code of Conduct • Deduction from Wages Sign Offs	Duration of employment and for 3 years for past employees. Contract to be retained for 7 years for a past employee.
Parental Leave Acts 1998 and 2006	• Parental Leave • Force Majeure	8 years from the date of the leave for both past and present employees.
Protection of Young Persons (Employment) Act 1996	• Records of age for those under 18 years of age	3 years from date of creation for both past and present employees.
Companies Acts and Taxes Consolidation Act 1997	• Records of tax payment	6 years for both past and present employees. This will be the responsibility of payroll.
Companies Act 2014	• Accounting records	7 years after the end of the financial year for both past and present employees.
Safety Health and Welfare at Work Act (General Applications) 1993	• Records of Accidents and dangerous occurrences.	10 years from the date of the accident for both past and present employees.
	• Disciplinary Records	For present employees, the duration of the sanction is 12 months. However, there is justification in retaining the sanction if there is a continuation of the poor performance. In the case of a sequence of sanctions up to and including dismissal, the company reserve the right to retain this

		sequence to illustrate the fair process conducted by the Company should a case be taken against the Company. For past employees, retention of the file for a duration of 3 years.
	Grievance Records	For present employees, the duration of the grievance procedure, founded or otherwise is 12 months. For past employees, retention of the file for a duration of 3 years.
	Absence Records	Absence records must be retained for a duration of 12 months. However, these records will be retained by Payroll for a longer duration.
	- Passports - Birth Certs - Drivers Licenses	Should be verified at recruitment stage to ensure the employee is permitted to work in Ireland but it should not be stored on the system. A copy of the driver's licence (if any) should be forwarded to the insurance company/car company.
The Protection of Employment Acts 1977—2007	Collective Redundancies	3 Years