# DATA PROTECTION ACT[1]

The Data Protection Acts 1988 to 2018 regulate the way in which companies may use the personal information of individuals and prohibits the unauthorised use or disclosure of that information.
It is the Company's policy to comply with its legal obligations in this regard.
The purpose of this document is to advise employees of the conditions surrounding the use and recording of employee personal data by the Company.

This document sets out the conditions surrounding the collection, processing and storage of data relating to employees.

- Employees must inform the Human Resources Department of any changes to their personal details (for example, change of address etc).
- Supervisors and management must forward all personal information held about employees to the HR Department.
- The Human Resources Department is responsible for the review and updating of this policy and bears overall responsibility for ensuring compliance with data protection legislation.
- The Data Protection Officer for the Company is the Finance Manager.

This policy has been drafted in accordance with the Data Protection Acts 1988-2018.

**DEFINITIONS**
See Glossary of Terms.

**Collection and Storage of Information**

The Company processes personal data relating to its employees in the course of business in a variety of circumstances e.g. recruitment, training, performance reviews, and administration of benefits and to protect the legitimate interests of the Company.

Processing of data includes collecting, recording, storing, altering, disclosing, and destroying data. This policy covers any individual about whom The Company processes data. This may include potential employees (during the recruitment and selection process), current and former employees.

Information which is usually obtained includes cvs, interview notes, ability test results, references and other pre-employment screening checks, medical checks, bank account details, personal details necessary for the administration of benefits such as pay, pensions, medical or performance records, corrective action records, grievance records, training records, biometric data (outline of finger print) and/or photographs for access and time and attendance records etc. (This list is not exhaustive.)

[1] Not reviewed by William Fry. Awaiting instructions from Sarah Murphy re drafting of Data Privacy Notice

Personal information kept by The Company will normally be stored on the employee's personal manual file and the HR electronic database in Ireland in accordance with this data protection policy and the Data Protection Acts 1988-2018 (Prior to the purchase by the Company of a HR Database, softcopy information will be retained in Excel files which will either be password protected or encrypted).

Where it is necessary to obtain personal information relating to any individual, The Company will ensure that information is:

- Obtained and processed fairly
- Retained for one or more specified, explicit and lawful purpose(s)
- Used and disclosed in a manner/s compatible with the purpose/s for which it was obtained
- Kept safe and secure
- Kept accurate, complete and up-to-date
- Adequate, relevant and not excessive
- Retained for no longer than is necessary for the purpose/s for which it was obtained; ***and***
- Furnished to an employee (to whom it relates) on request

Personal information will normally be obtained directly from the employee concerned. However, in certain circumstances it may be necessary to obtain information from third parties e.g. references from previous employers etc.

Personal information kept by The Company shall normally be stored on the employee's personnel file which is located in the HR Department. Access to this database (hard and soft copy) is restricted to authorised personnel.

Highly sensitive information such as medical reports obtained during the course of your employment, medical certificates etc will be stored on the employee's personal file in the HR Department. The Company will ensure that only authorised personnel have access to the employee's personnel file.

It may be necessary to store certain other information outside the HR Department. The employee's manager may have access to certain personal information where necessary, for example, absence records, medical reports etc.

Personal information collected by the Company is used for ordinary personnel management purposes. Where there is a need to collect information for another purpose, the Company shall inform you of this.

Employees are responsible for ensuring that they inform HR of any changes in their personal details, i.e., change of address etc. Employees must inform the HR Department of any changes in employee's personal details. The Company will endeavor to ensure personal data held by the Company is up to date and accurate.

The Company is under a legal obligation to keep certain information for a specified period of

time. In addition the Company will need to keep personnel information for a period of time in order to protect its legitimate business interests.

**Security and Disclosure of Information**

The Company shall take all reasonable steps to ensure that appropriate security measures are in place to protect the confidentiality of both electronic and manual information. Security measures will be reviewed from time to time having regard to the technology available, the cost and the risk of unauthorised access. Employees must implement all security policies and procedures e.g. use of computer passwords, locking filing cabinets etc.

HR information will only be processed for employment related purposes and in general will not be disclosed to third parties except where required or authorised by law or with the agreement of the employee. HR files are stored in the HR Department and authorised employee/s that has access to those files must ensure that they treat them confidentially. Employees working in the payroll department/accounts must treat all information they receive confidentially and must not disclose it, except in the course of their employment.

All employees will have access to a certain amount of personal data relating to customers, colleagues or third parties. Employees must play their part in ensuring its confidentiality. They must adhere to the data protection principles and must not disclose such information, except where necessary in the course of their employment, or in accordance with the law. They must not remove or destroy personal information except for lawful purposes. If an employee is in any doubt regarding their obligations they should contact the HR Department or the Data Protection Officer (Finance Manager).

Any breach of the data protection principles is a serious matter and may lead to corrective action up to and including termination of employment.

**Medical Information**

The Company may request that interview candidates attend a Medical Practitioner for examination. The purpose of the report/examination is to determine an employee's fitness or otherwise to do the job for which they are being considered. The information will not be used for any other purpose. A copy of the medical report will be retained and stored in the Human Resources Department.

Occasionally, it may be necessary for the Company to refer an employee to a Company nominated doctor during the course or his/her employment. The Company will request permission from the employee concerned to receive and retain a copy of the medical report from the examining doctor. This report will be received by the HR Department and will then be retained on the employee's personal file. The contents of the report may be disclosed to the employee's immediate manager. All copies of medical certificates submitted to the Company during an employee's absence, including return to work certificates will also be retained on the employee's personal file.

Employees are entitled to request access to their medical reports. Should an employee wish

to do so, please contact the HR Department who will consult with the doctor who examined you. The final decision lies with the doctor to decide whether the information should be disclosed to you or not in accordance with SI No. 82 of 1989.

**Interview Records**

The Company will retain records of application forms, cvs, interview notes, ability tests, references etc in order to ensure compliance with the Employment Equality Acts 1998- 2015 and with the Company's Equal Opportunities Policy for a period of 18 months.

**Email Monitoring**

The Company provides email facilities and access to the internet. In order to protect against the dangers associated with email and internet use, screening software is in place to monitor email and web usage. Please refer to the Company's Email and Internet Policy for further details. Note in particular that the Company may open your mailbox upon specific authorisation by a manager in cases where there is a suspicion of inappropriate use or screening equipment or a complaint indicates that a particular mailbox may contain material which is dangerous or offensive or where there is a legitimate work reason or in the legitimate interests of the Company

**Giving References**

The Company will seek the express written consent of a former employee before giving a reference in relation to that former employee unless the requesting party can provide evidence to The Company that the former employee has given written consent to the disclosure of information in relation to him or her. A guideline on issuing and obtaining references has been made available to managers.

**Data Protection Officer**

The Finance Manager is the Data Protection Officer for the Company. He/She bears overall responsibility for ensuring compliance with data protection legislation. All employees must co-operate with the Data Protection Officer when he/she is carrying out his/her duties in accordance with data protection laws and policies.

**Access Requests**

Employees are entitled to request information held about them on computer or on their manual personal file in accordance with data protection legislation. The Company will provide this information within 40 days.

An employee should make a request in writing to the Data Protection Officer stating the exact information required.

Employees are only entitled to information about them and will not be provided with information relating to other employees or third parties.

Information which is classified as an 'opinion' or an expression of a view will not be provided where it is classified as confidential.

An employee who is dissatisfied with the outcome of an access request has the option of using the Company Grievance Procedure.

**Right to Object**

Employees have the right to object to data processing which is causing them distress. Where such objection is justified, the Company will cease processing that information unless it has a legitimate business interest that prevents this. The Company will make every effort to alleviate the distress caused to the individual.

An objection must be made in writing to the Data Protection Officer, outlining in detail the nature of their objection and grounds for same and the harm being caused to the employee.

**Transmission of Data Outside of the State**

As the Company operates internationally, it may be necessary in the course of business to transfer employee's personnel information within the Company and to other group companies outside the EEA, which do not have comparable data protection laws as Ireland. The transfer of such information is necessary for the management and administration of your contract of employment and to facilitate the overall administration of personnel within the group of companies. When this is necessary, the Company will take steps to ensure that the information has the same level of protection as it does in this State. The Company will only transmit to other sites which agree to guarantee this level of protection.

This policy will be reviewed from time to time and may be amended or withdrawn depending on changes in the law or the experience of the policy in practice. If you have any further questions on data protection, please contact Janine McNamara, Data Protection Officer for the Company.

## Glossary of Terms

**Personal Data**
Data relating to a living individual (who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller)

**Processing Data**
To 'process' such personal data means:

- obtaining, recording or keeping the information, or
- collecting, recording, organising, storing, altering or adapting the information or data,
- retrieving, consulting or using the information or data,
- disclosing the information or data by transmitting, disseminating or otherwise making it available, or
- aligning, combining, blocking, and erasing the information or data.

**Data Controller**
A Data Controller is a person who, either alone or with others, controls the contents and the use of personal data.

**Principles of Data Protection**

1. The data must be obtained and processed fairly.
2. The data should be accurate, complete and kept up to date.
3. The data shall be obtained for one or more specified, explicit and legitimate purpose(s).
4. The data shall not be further processed in a manner incompatible with that purpose(s).
5. The data shall be adequate, relevant and not excessive in relation to the purpose(s) for which it was collected.
6. The data shall not be kept for longer than is necessary for that purpose(s).
7. Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.

**Sensitive Personal Data**

'Sensitive Personal Data' includes information about a person's:

1. Racial or ethnic origin, political opinions, religious or philosophical beliefs;
2. Trade union membership;
3. Physical or mental health or condition, or sexual life;

4. Commitment or alleged commitment of an offence or any proceeding for an offence committed or allegedly committed by the data subject, the disposal of such proceedings or the sentence of any court proceedings.