# GDPR POLICY

GENERAL DATA PROTECTION REGULATION

## INTRODUCTION

The General Data Protection Regulation, part of the Data Protection Bill comes into force on 25th May 2018. The GDPR 2018 (the Act) contains principles affecting employees' and other personal records. Information protected by the Act includes not only personal data held on computer but also certain manual records containing personal data, for example employee personnel files that form part of a structured filing system. The purpose of these rules is to ensure that you do not breach the Act and that you understand the Company's policy on handling protected data.

## PURPOSE

The Company is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out the Company's commitment to data protection, and your rights and obligations in relation to personal data.

## SCOPE

This policy applies to the personal data of job applicants, employees, workers, contractors and former employees, referred to as HR-related personal data.
Questions about this policy, or requests for further information, should be directed to the HR Department.

## DEFINITIONS

**"*Personal data*"** is any information that relates to an individual who can be identified from that information.
**"*Processing*"** is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.
**"*Special categories of personal data*"** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.
**"*Criminal records data*"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

## DATA PROTECTION PRINCIPLES

The Company processes HR-related personal data in accordance with the following data protection principles:

- The Company processes personal data lawfully, fairly and in a transparent manner;
- The Company collects personal data only for specified, explicit and legitimate purposes;
- The Company processes personal data only where it is adequate, relevant, and limited to what is necessary for the purposes of processing;
- The Company keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay;
- The Company keeps personal data only for the period necessary for processing (see Data Retention Policy) and
- The Company adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage;

The Company will tell you the reasons for processing your personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data related to you for other reasons.

Where the Company processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with the relevant legislation on special categories of data and criminal records data.

We will update all HR related data promptly if you advise us that it is inaccurate.

Personal data gathered during your employment is held in your HR file and on its HR systems. The periods for which the Company holds HR-related personal data are contained in the Data Retention Policy.

## LAWFUL BASIS FOR MAINTAINING DATA

The Company will maintain electronic and manual records relating to all employees. The Company will only hold data it deems necessary for the purposes of managing the employment relationship, complying with relevant legislation and with terms of the employment contract.

## CONSENT

By signing the Statement of Terms and Conditions of Employment and the Staff Handbook or applying for employment with the Company, you give your consent to the Company using personal data and sensitive data which relates to you and/or identifies you, for the purposes of administering this agreement, administering your pay and other benefits, reviewing your performance, undertaking disciplinary action and other action in relation to you, maintaining appropriate employee records, providing references in relation to you, and managing its business. For more information see the Employee Privacy Notice available in the Staff Handbook.

You have the right to apply to withdraw your consent at any time. A withdrawal request should be made in writing to the HR Department. Any such application will be considered in line with the requirements of the GDPR and the Company's requirement to use the data to carry out its duties as an employer.

## INDIVIDUAL RIGHTS

As a data subject, you have a number of rights in relation to your personal data.

## SUBJECT ACCESS REQUESTS

You have the right to make a subject access request. If you make a subject access request, the Company will tell you:

- whether or not your data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from you;
- to whom your data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long your personal data is stored;
- your right to rectification or erasure of data, or to restrict or object to processing;
- your right to complain to the Information Commissioner if you think the Company has failed to comply with your data protection rights; and
- whether or not the Company carries out automated decision-making and the logic involved in any such decision-making.

The Company will also provide you with a copy of the personal data undergoing processing. This will normally be in electronic form if you have made a request electronically, unless you agree otherwise.

## MAKING A REQUEST

To make a subject access request, you should send the request to the HR Department. The Company will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the Company processes large amounts of the individual's data, it may respond within three months of the date the request is received. The Company will write to you within one month of receiving the original request to tell you if this is the case. If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, the Company can agree to respond but will charge a fee, which will be based on the administrative cost of responding to your request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Company has already responded, and you will be notified that no further response will be provided.

## OTHER RIGHTS

You have a number of other rights in respect of your personal data. You can ask the Company to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if your interests override the Company's legitimate grounds for processing data (where the Company relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether your interests override the Company's legitimate grounds for processing data.

To ask the Company to take any of these steps, the individual should send the request to the HR Department.

## DATA SECURITY

The Company takes the security of HR-related personal data seriously. The Company has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. Where the Company engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and Company measures to ensure the security of data.

## DATA BREACHES

If the Company discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The Company will record all data breaches regardless of their effect.
If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

## INTERNATIONAL DATA TRANSFERS

The Company will not transfer HR-related personal data to countries outside the EEA.

## EMPLOYEE PRIVACY NOTICE

An Employee Privacy Notice is made available to all staff within the Staff Handbook.