Croner

Sample Data Protection Policy

Aim & Scope of Policy

We collect and use information about our employees. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means. We fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR) for the processing of personal data, which includes special categories of data.

Where third parties process data on behalf of the Company, the Company will ensure that the third party takes such measures in order to maintain the Company's commitment to protecting data.

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

Types of Data Held

We keep several types of personal data aon our employees in order to carry out effective and efficient processes, as follows:

- Name, address, phone numbers of employees.
- Name, address, phone numbers of employees' emergency contact.
- CVs and other information gathered during recruitment.
- References from former employers.
- National Insurance numbers.
- Tax codes.
- Terms and conditions of employment.
- Job title, job descriptions and pay grades.
- Conduct issues such as letters of concern, disciplinary proceedings.
- Training details.
- Holiday records.
- Job performance information.
- Sickness absence records.
- Medical or health information.

Data Protection Principles

All personal data obtained and held by the Company will:

- Be processed fairly, lawfully and in a transparent manner.
- Be collected for specific, explicit, and legitimate purposes.
- Be adequate, relevant and limited to what is necessary for the purposes of processing.
- Be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay.
- Not be kept for longer than is necessary for its given purpose.
- Be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures.
- Comply with the relevant GDPR procedures for international transferring of personal data.

Employees have the following rights in relation to their personal data:

- The right to be informed.
- The right of access.
- The right for any inaccuracies to be corrected.
- The right to have information deleted.
- The right to restrict the processing of the data.
- The right to portability.
- The right to object to the inclusion of any information.
- The right to regulate any automated decision-making and profiling of personal data.

Procedures

The Company has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- It appoints or employs employees with specific responsibilities for:
  - **a.** The processing and controlling of data.
  - **b.** The comprehensive reviewing and auditing of its data protection systems and procedures.
  - **c.** Overviewing the effectiveness and integrity of all the data that must be protected.
- Training of relevant members of staff who are responsible for processing data.
- It can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with.
- It carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security.
- It has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches and understands the requirement to report certain breaches to the ICO.
- It is aware of the implications of international transfer of personal data.

Data Disclosures

The Company may be required to disclose certain data, the reasons for which include:

- Any employee benefits operated by third parties including insurance policies.
- For Statutory Sick Pay purposes.
- HR management and administration.

These kinds of disclosures will only be made when strictly necessary for the purpose.

Data Security

The Company adopts procedures designed to maintain the security of data when it is stored and transported.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by the Managing Director. Where personal data is recorded on any such device it will be adequately protected.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

International Data Transfers

The Company does not transfer personal data to any recipients outside of the EEA.

Breach Notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the Company becoming aware of it and may be reported in more than one instalment.

Training

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

Records

The Company keeps records of its processing activities including the purpose for the processing and retention periods in its HR Data Record. These records will be kept up to date so that they reflect current processing activities.

Disclaimer:

Croner Group Ltd is not liable for any errors or omissions in the template and shall not be liable for any loss, injury or damage of any kind caused by its use. Use of the template is entirely at the risk of the User and should you wish to do so then independent legal advice should be sought before use.

Use of the template will be deemed to constitute acceptance of the above terms.