The General Data Protection Regulation 2018 (GDPR)

Aim and Scope of Policy

This policy applies to the processing of personal data in both manual and electronic records held by ERP Security Ltd in connection with its human resources function, as described below. It also covers the Company's response to any data breach and other rights under the General Data Protection Regulation.

This policy applies to the personal data of job applicants, current and former employees, apprentices, volunteers, placement students, workers, and self-employed contractors. These individuals are referred to as 'relevant individuals' in this policy.

"Personal data" refers to any information that can identify an individual, either directly or indirectly, such as a person's name, identification number, location, or online identifier. It may also include pseudonymised data.

"Special categories of personal data" includes information related 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 (when used for identification purposes).

"Criminal offence data" relates to an individual's criminal convictions and offences.

"Data processing" refers to any operation or set of operations performed on personal data, whether automated or manual, such as collection, recording, organisation, storage, alteration, retrieval, use, disclosure, erasure, or destruction.

ERP Security Ltd is committed to ensuring that personal data, including special categories of personal data and criminal offence data (where applicable), is processed in compliance with GDPR and domestic laws. All employees are expected to adhere to this policy and related procedures. Where third parties process data on behalf of ERP Security Ltd, the Company will ensure that those parties maintain similar data protection standards.

ERP Security Ltd acknowledges its responsibility for the processing, management, regulation, and retention of all personal data held, whether in manual records or electronic formats.

Types of Data Held

Personal data is retained in personnel files or within the Company's HR systems. The types of data that may be held by the Company include:

- Name, address, phone numbers (including next of kin)

- CVs and recruitment information
- References from former employers
- National Insurance numbers
- Job titles, descriptions, and pay grades
- Records of conduct issues (e.g., letters of concern, disciplinary actions)
- Holiday records
- Internal performance information
- Medical or health information
- Sickness absence records
- Tax codes
- Terms and conditions of employment
- Training details

Data Protection Principles

All personal data held by ERP Security Ltd will be:

- Processed fairly, lawfully, and transparently
- Collected for specified, legitimate purposes
- Adequate, relevant, and limited to what is necessary for processing
- Accurate and kept up to date; inaccurate data will be rectified or erased promptly
- Retained for no longer than necessary
- Processed securely to protect against unauthorised or unlawful processing, loss, destruction, or damage, using appropriate technical and organisational measures
- Transferred in accordance with GDPR provisions for international data transfers

In addition, personal data will be processed in recognition of individuals' rights, including:

- The right to be informed
- The right of access
- The right to rectification (correction of inaccuracies)

- The right to erasure (deletion)
- The right to restrict processing
- The right to data portability
- The right to object to processing
- The right to regulate automated decision-making and profiling

Procedures

ERP Security Ltd takes the following steps to protect the personal data it holds:

- It designates employees responsible for data processing and control, overseeing audits and reviews of data protection systems and procedures.
- It provides information to employees about their data protection rights, how their data is used, and the steps they can take if they believe their data has been compromised.
- It offers training to employees on data protection, confidentiality, and how to treat personal information securely.
- It tracks all personal data held, its origins, and who it is shared with.
- It conducts risk assessments to identify vulnerabilities in data handling and take corrective measures to mitigate risks.
- It seeks explicit consent from relevant individuals for processing their data, ensuring consent is freely given, informed, specific, and unambiguous. Consent can be withdrawn at any time.
- It has mechanisms in place to detect, report, and investigate data breaches and to notify the Information Commissioner's Office (ICO) of significant breaches.

Access to Data

Relevant individuals have the right to be informed about the processing of their personal data and to request access to this data. Requests for access should be submitted using the appropriate form available from the HR Department. The request should be made to the HR Manager, TBC.

- ERP Security Ltd will not charge for data access requests unless they are manifestly unfounded, excessive, or repetitive.
- The Company will respond to access requests without undue delay and within one month, with a possible extension of up to two months for complex requests.

If individuals believe their data is inaccurate, they should inform ERP Security Ltd immediately, and steps will be taken to correct it.

Data Disclosures

Certain data may be disclosed to third parties under specific circumstances, such as:

- Employee benefits administered by third parties
- Health data for health and safety or occupational health requirements
- Statutory Sick Pay
- HR management to assess job performance or health-related issues
- Employee insurance or pension plans

These disclosures will only occur when strictly necessary.

Data Security

ERP Security Ltd adopts strict security measures to protect data during storage and transfer. Employees must ensure that confidential data is securely stored and not accessible to unauthorised individuals.

Employees must:

- Ensure that confidential information is stored securely and accessed only by authorised persons.
- Avoid leaving confidential data exposed to unauthorised viewing.
- Use passwords to protect computer systems and avoid sharing them.
- Use screen blanking on computers to prevent unauthorised access.
- Avoid storing personal data on laptops, USB drives, or similar devices, unless authorised.

Where personal data is stored on such devices, encryption must be used to ensure security.

Failure to comply with these security measures may result in disciplinary action.

International Data Transfers

ERP Security Ltd does not transfer personal data outside the EEA.

Breach Notification

In the event of a data breach that poses a risk to individuals' rights and freedoms, the breach will be reported to the ICO within 72 hours of discovery. Affected individuals will be informed if the breach is likely to cause significant harm. Public notification will occur if the breach is substantial.

Training

New employees are required to read and understand the data protection policies as part of their induction. Ongoing training ensures that all employees are aware of their responsibilities under GDPR, including actions to take in case of a data breach.

Records

ERP Security Ltd maintains records of its data processing activities, including the purpose of processing and retention periods. These records will be regularly reviewed to reflect current processing activities.

Data Protection Officer

The Company's Data Protection Officer is Eric Manangu, CEO.