RSG
Railsafe Group

Business Management System

Section 12: Human Resources

Part 2 – Data Protection Policy

Document Record		
Rev	Changes	Date
1	Original	1st September 2023
2	Review	30th August 2024
3	Amendment	27th September 2024
4	Review	29th August 2025

Data Protection Policy

1. Introduction

In the course of your work, you may come into contact with or use confidential information about employees, temporary workers, contractors, clients, and customers, for example, their names, home addresses, and other personal details. The UK Data Protection Act 2018 and General Data Protection Regulation (GDPR) set out principles affecting the handling of personal data. Information protected by this legislation includes personal data held on computers and certain manual records, such as personnel files that form part of a structured filing system. The purpose of this policy is to ensure that you comply with the law. If you are in any doubt about what you can or cannot disclose and to whom, seek advice from the Data Protection Officer (DPO) before taking any action.

You should be aware that under data protection law, you are personally accountable for your actions and can be held liable if you knowingly or recklessly breach the law. Any serious breach of data protection legislation will also be regarded as misconduct and will be dealt with under the company's disciplinary procedures. Unauthorised access to personal records constitutes gross misconduct and could lead to summary dismissal.

2. The Data Protection Principles

Railsafe Group and all its employees must comply with the six core data protection principles outlined in the GDPR at all times when processing personal data. These principles require that personal data must be:

2.1 Lawful, fair, and transparent

Processed lawfully, fairly, and in a transparent manner in relation to the data subject. Personal data must not be processed unless a lawful basis for processing is met, such as consent, contractual necessity, legal obligation, or legitimate interest.

2.2 Collected for specified, explicit, and legitimate purposes

Personal data must only be collected for specified purposes and must not be processed further in a manner that is incompatible with those purposes.

2.3 Adequate, relevant, and limited to what is necessary

Personal data must be limited to what is necessary for the purposes for which they are processed. The company will regularly review records to ensure that no excessive or unnecessary data is being held.

2.4 Accurate and kept up to date

Reasonable steps must be taken to ensure personal data is accurate and kept up to date where necessary. Employees, temporary workers, and contractors must promptly inform their line manager of any changes to their personal information.

2.5 Retained only for as long as necessary

Personal data must not be kept for longer than necessary for the purposes for which it is processed. Railsafe Group has a data retention policy to ensure that data is only held for appropriate periods. For example, personnel files will be retained for up to **six years** after termination of employment or contract, unless required for legal or operational purposes.

2.6 Processed with appropriate security

Appropriate technical and organisational measures must be taken to ensure the security of personal data. This includes protecting data against unauthorised or unlawful processing, accidental loss, destruction, or damage.

3. Lawful Bases for Processing Personal Data

Railsafe Group processes personal data on the following lawful bases under the GDPR:

- **Contractual necessity**

  Data is processed to fulfil employment or contractual obligations.

- **Legal obligation**

  Data is processed to comply with legal obligations.

- **Legitimate interests**

  Data is processed in the legitimate interests of the company, provided this does not override the rights and freedoms of individuals.

- **Consent**

  For specific purposes where required, consent may be sought from individuals for the processing of their data.

Sensitive personal data (e.g., health records, racial or ethnic origin) may only be processed where there is explicit consent or another lawful basis under the GDPR.

4. Employee, Temporary Worker, and Contractor Consent to Personal Data Processing

By signing your employment contract (employees), contractor agreement (contractors) or registration form (contractors and temporary workers), you consent to the processing of your personal data for the purposes of your employment or contract, including payroll, HR administration, and business continuity planning. Consent is a condition of employment/engagement, but wherever possible, the company will rely on legitimate interests or legal necessity as the lawful basis for processing.

5. Your Rights as a Data Subject

Under the GDPR, employees, temporary workers, and contractors have the following rights regarding their personal data:

5.1 The right to access

You have the right to access personal data that Railsafe Group holds about you. To request access, you must submit a written request. Railsafe Group may charge a reasonable fee for excessive, repetitive, or unfounded requests.

5.2 The right to rectification

You have the right to request that inaccurate or incomplete personal data is corrected.

5.3 The right to erasure

You have the right to request that personal data be erased when it is no longer necessary for the purposes for which it was collected, or if the data is processed unlawfully.

5.4 The right to restrict processing

You have the right to request the restriction of processing where there is a dispute over the accuracy of the data or if processing is unlawful.

5.5 The right to data portability

Where data is processed by automated means, you have the right to request the transfer of your personal data to another organisation.

5.6 The right to object

You have the right to object to the processing of your personal data for certain purposes, such as direct marketing.

5.7 Rights related to automated decision-making and profiling

You have the right to request human intervention in decisions made solely by automated means if those decisions significantly affect you.

6. Data Security

Railsafe Group has implemented appropriate technical and organisational measures to ensure the security of personal data. Personal data held in physical form must be stored in locked filing cabinets, and access is restricted to authorised personnel only. Data held electronically must be protected by passwords, encryption, or other suitable security methods. Access to data is limited to those who require it to perform their job duties.

Personal data must not be removed from company premises without authorisation. When working remotely, employees must ensure that personal data is kept secure at all times.

7. Data Breaches

In the event of a data breach, Railsafe Group will promptly assess the risk to individuals' rights and freedoms. If there is a significant risk, the breach will be reported to the Information Commissioner's Office (ICO) within 72 hours. Affected individuals will also be notified if the breach is likely to result in a high risk to their rights and freedoms.

8. International Data Transfers

Railsafe Group will not transfer personal data to countries outside the UK or EEA unless adequate protections are in place to safeguard the data, in accordance with GDPR requirements.

9. Your Obligations in Relation to Personal Data

If your role involves processing personal data, you must ensure that you comply with this policy and the GDPR. This includes ensuring that data is:

- Processed only for the purposes for which it was collected.
- Kept secure at all times.
- Not disclosed to unauthorised persons.

You must verify the identity of individuals requesting access to personal data and follow company procedures for secure transmission of data.

10. Complaints

If you believe that your personal data has not been handled in accordance with this policy, you may raise the issue with the Data Protection Officer. If the issue is not resolved to your satisfaction, you may escalate it as a formal grievance under Railsafe Group's grievance procedure.

RSG
Railsafe Group

11. Compliance

Compliance with this policy is mandatory for all employees. Failure to comply may result in disciplinary action, including dismissal for gross misconduct. Criminal liability may also apply in cases of unlawful data processing.

If you have any questions about this policy or data protection in general, please contact the Data Protection Officer (DPO).

Jamie Spinks, Director **29th August 2025**