Data Protection Policy

Release Certificate	
Status of this Document:	Published
Document Version:	**1.1**
Release Date:	**31/05/2022**

Table of Contents

1 OVERVIEW

ScotRail Trains processes personal data in order to deliver a range of services, as an employer and to engage with a range of other stakeholders. This policy outlines how we meet our obligations under current data protection legislation, including the Data Protection Act (2018) (DPA) and the UK General Data Protection Regulation (UK GDPR).

The Privacy and Electornic Communications Regulations (PECR) sit alongside this legislation. The regualations cover marketing, cookies and electronic communications and also form part of the data protection legislation.

We must comply with data protection legislation and be able to evidence our compliance. We must process personal data safely and securely, minimising risk to individuals. We also make provision for data subjects to exercise their rights under the legislation.

The Information Commissioner's Office (ICO) is the UK regulator for data protection matters.

2 PURPOSE

The purpose of this policy is to provide a clear statement of principles, values and standards in respect of data protection. This policy is intended to ensure that we consistently act to protect data subjects' interests and personal data whilst remaining compliant with data protection legislation.

3 SCOPE

This policy is applicable to all personal data processed by ScotRail whether on our premises or elsewhere. It applies to everyone working for ScotRail, including employees, agents and contractors.

'Processing' of data includes any instance of personal information being handled.

4 POLICY STATEMENT

The company is fully committed to data protection principles.

We undertand our responsibilites for, and will be able to demonstrate compliance with, the six principles set out in the UK GDPR.

We maintain an internal governance framework which regularly monitors and assesses our compliance with our data protection obligations, and ensures that any opportunities to improve performance are recognised and acted upon. We continuously record our personal data records and processing activities, communicate clearly and openly with data subjects, and conduct data protection impact assessments whenever significant changes are made to how we process data. This ensuresthat we are taking appropriate measures to safeguard personal data and the rights and interests of data subjects. We operate a defined reporting mechanism to ensure the timely and effective notification to the Information Commissioner's Office (and other relevant authorities) of any breach.

4.1 Definitions

"Personal data" is information that relates to an identified or identifiable living individual.

"Special category data" is personal data which is more sensitive, and requires greater protection. Special category data can only be processed in more limited circumstances.

The types of special category data are:

- race
- ethnic origin

• politics
• religion
• trade union membership
• genetics
• biometrics (where used for ID purposes)
• health
• sex life
• sexual orientation
Criminal offence data is treated similarly to special category data.

“Data processing” includes any action taken during the lifecycle of personal data, including creating, storing and disposing of data.

“Data Controller” – an organisation that determines the purposes and means of processing personal data.

“Data Processor” - is responsible for processing personal data on behalf of, and in accordance with instructions given by, a controller.

4.2 Data Protection Principles

Principle One – Lawfulness, fairness and transparency

Before we process any personal data, we ensure that an appropriate legal basis under Article 6 of the UK GDPR has been identified and documented. These are:

- Consent of the data subject
- Processing in our legitimate interests and this is not overridden by the rights and freedoms of the data subject. Public authorities cannot rely on legitimate interests for any processing where we are performing our tasks as a public authority.
- Where necessary to meet a legal obligation
- To fulfil a contract or pre-contractual obligation
- To protect someone’s vital interests (“life or death” situations)
- To fulfil a public task, or acting under official authority

We only process special category personal data where we also have a second legal basis for doing so under Article 9 of the UK GDPR. We require a basis in law to process this type of data or we require additional conditions from Schedule 1 of the DPA to be met.

UK GDPR Condition	**Schedule 1 Condition**
Explicit consent	
Employment, social security and social protection	+ Condition 1
Vital Interests (life or death)	
Not for profit bodies (membership data)	
Manifestly made public by the data subject	
Legal claims or judicial acts	
Substantial public interest	+ one of Conditions 6-28
Health or social care	+ Condition 2
Public health	+ Condition 3
Archiving, research, statistics	+ Condition 4

At the point of data collection (or as soon as practicable thereafter), we provide the data subject with ‘fair processing information’ in our privacy notice, available on our website.

Our privacy notices are designed to offer transparency to data subjects, thereby affording genuine control and choice over how their personal data are processed.

Principle Two – Purpose limitation

We only process personal data for purposes which are lawful and compatible with those which we declared when the data was collected. If we need to use personal data for a different purpose, we inform data subjects.

Principle Three – Data minimisation

We keep our personal data to a minimum and never hold it on a 'nice to have' or 'just in case' basis. We destroy any personal data that we receive but cannot legitimately process.

Principle Four – Accuracy

We take reasonable steps to ensure that personal data is kept accurate and up to date, and rectify inaccurate data when we are made aware of it.

Principle Five – Storage limitation

Our internal procedures enable us to identify the nature and location of stored personal data and to securely dispose of itwhen no longer required, in line with our internal data classification and retention policies. We conduct periodic reviews of data stores to ensure that we are not retaining any data that are no longer required.

Principle Six – Security, integrity and confidentiality

We assess the security risk associated with each of our data processing activities and take steps to ensure that relevant and proportionate controls are put in place andoperate effectively to protect the confidentiality, integrity and availability of personal data. Measures include IT/technical, physical and organisational measures.

4.3 Accountability and Governance

We need to demonstrate and be able to evidence how we comply with the legislation and follow the principles above. There are a number of ways we do this, including:

- Training and awareness
- Documentation such as Personal Data Asset registers, Records of Processing Activities and logs of data subject requests
- Risk management, including Data Protection Impact Assessments
- Compliant procurement practices
- Formal change management processes that include review of data protection considerations, and the embedding of a 'privacy by design and default' culture

We regularly monitor and review our controls and ensure we can evidence good practice in complying with the legislation.

The company's aggregated data security risk is recorded within our company risk register and proactively managed in accordance with our established risk management framework.

4.3.1 Data Protection Officer

ScotRail has a Data Protection Officer, with formalised respsonsibilities. We recognise that the DPO role must remain independent of any data processing activities and have sufficient authority to act in a robust and independent manner

.

4.4 Data Subjects' Rights (DSRs)

We recognise that data subjects have a number of rights (DSRs):

- **Access**: to establish whether we hold any of their personal data and to request access to their data
- **Rectification**: to request that inaccurate or incomplete information is amended
- **Erasure**: the 'Right to be Forgotten' applies in certain circumstances, e.g. withdrawing consent where that is the legal basis for processing
- **Restriction of Processing**: to request that processing is restricted or suspended where data inaccuracy is suspected, or processing is unlawful but the individual opposes data deletion
- **Portability**: to obtain a copy of their data in a commonly used format and have it transferred to another data controller
- **Objection**: to request the cessation of processing that is being conducted on the grounds of 'legitimate interest' or as part of direct marketing activities
- **Automated Decision Making**: to object to any significant decisions being taken solely by automated means and to require an element of human intervention, an opportunity to express a counter point of view and an explanation as to how the decision was ultimately reached

We maintain procedures to enable us to respond to any DSR application in a full, timely and compliant manner, acknowledging the minimum requirement to offer our response within one month of receiving the request. Staff must be able to recognise a DSR request and pass it on without delay to the Data Protection inbox so it can be centrally logged and processed according to legislative requirements.

4.5 Complaints Handling

If a data subject is dissatisfied with any aspect of our processing or our response to a DSR request, they can request an internal review. If they are still dissatisfied, they may complain to the regulator, the ICO.

4.6 International Transfers

Wherever possible we do not transfer personal data outwith the UK or EEA. Where this is essential, we ensure appropriate safeguards are in place and inform data subjects via privacy notices. The DPO is involved in any decision surrounding international data transfres.

4.7 Data Breach and Incident Management

A data breach occurs when personal data is accidentlly disclosed, lost or made unavailable. We require all data breaches, and 'near misses', to be reported, recorded and investigated. Further information and reporting forms are made available on the Intranet. Outcomes and lessons learned are centrally logged to promote organisational learning and improvement.

Where the regulatory criteria are met, we report incidents ot the ICO within 72 hours of becoming aware of them, and inform data subjects as appropriate.

4.8 Children's data

Where we process any children's personal data during the normal course of business, such as ticket purchases, CCTV or incidents, we will process that personal data with an appropriate level of due care and attention. We do not require consent to process children's personal data in these cases, as we will rely on other legal conditions, such as fulfilment of a contract or vital interest.

5 POLICY ENFORCEMENT

This policy applies to every director, officer, employee, and sub-contractor of the company. Individuals must only process personal information in accordance with instructions provided to them and as part of their business role.

The Leadership Team enforce this policy. If we suspect a violation of this policy, we conduct an investigation to determine what action should be taken, which can involve disciplinary action.

This Policy does not form part of any contract of employment and it may be amended at any time. The latest version of the policy is available on both our Intranet and our website.

6 POLICY REVIEW

This policy will be reviewed when legislative changes occur or every three years.