| | |
|---|---|
| Document №: | 2454 |
| Version: | See IMS version history |
| Classification: | OFFICIAL |
| IMS Level: | 1 |

# Personal Data Handling Policy

# Document authorisation

| | Name | Position | Signature | Date |
|---|---|---|---|---|
| Prepared by | Roland George | Data Protection Officer | See document version history in IMS for evidence of approval. | 10/02/22 |
| Reviewed by | James Norman | SIRO | | 10/02/22 |
| Compliance Check by | Simon Henry | Head of Quality Management | | 10/02/22 |
| Endorsed by | Simon Blanchflower | CEO | | 10/02/22 |
| Approved by On behalf of EWRCo Board | Anne Baldock | Audit Committee Chair | | 10/02/22 |

# Revision history and summary of changes

| Change date | Version/Revision | Section | Change |
|---|---|---|---|
| 10/02/22 | V01 | Whole Document | First IMS Issue |

# Glossary

| Term | Description |
|---|---|
| automated decision-making | means the process of making a decision by automated means without any human involvement in making the decision (e.g. an employment candidate undertaking certain online assessments with predefined correct and incorrect answers and the application will be automatically accepted or rejected based on the candidates score). |
| controller | means the natural or legal person that determines the purposes and means of processing personal data (defined below), or EWR. This Policy only applies when EWR acts as a controller and not when the organization acts as a processor (defined below). |
| data breach | means a breach of security leading to the accidental, unlawful or unauthorised destruction, loss, alteration, disclosure of, or access to, personal data. |
| data subject | means any living individual whose personal data is collected, held or processed by an organisation. |
| data subject request | means data subject requests and objections made under the UK Data Protection Laws. |
| DPIA | means a data protection impact assessment. |
| European Guidelines | means the "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" (https://ec.europa.eu/newsroom/article29/items/611236/en). |
| ICO | means the UK Information Commissioner's Office. |
| personal data | means any information or opinion, whether true or not and whether recorded in a material form or not, about an identified individual or an individual who is reasonably identifiable, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to factors specific to the identity of that individual. |
| processor | means a natural or legal person that processes personal data (defined below) on behalf of a controller such as EWR's third-party vendors or affiliates, subsidiaries, and related corporate entities providing services. EWR may act as a processor in certain situations for affiliates, related corporate entities, and third parties. However, this Policy does not apply to EWR's personal data processing activities as a processor. If you have any questions about whether EWR is acting as a controller or a processor, please contact the Data Protection Office. |

| | |
|---|---|
| Processing | means any operation or set of operations performed on personal data, whether or not by automated means, such as collection, use, storage, dissemination, and destruction (and process and processed shall be construed accordingly). |
| Profiling | means any form of automated processing of personal data to evaluate aspects about a data subject. This includes, for example, predicating aspects about that individual's performance at work, economic situation, health, personal preferences, interests, behaviour, or location. |
| ROPA | means any of EWR's record of processing activities as required under Article 30 of the UK GDPR. |
| Special category data | means any data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (e.g. fingerprints), data concerning health and data concerning a natural person's sex life or sexual orientation together with information about a data subject's criminal convictions and offences. Even stricter protection must be applied to this data. |
| UK Data Protection Laws | means all applicable laws relating to privacy or data protection the United Kingdom, including the UK GDPR and the Data Protection Act 2018. |
| UK GDPR | means the EU General Data Protection Regulation (Regulation (EU) 2016/679) as it forms part of the laws of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended. |

# Table of contents

# 1. Introduction

1.1. East West Railway Company Limited ("EWR") is committed to being transparent about how it collects and uses data.

# 2. Purpose

2.1. This personal data handling policy ("Policy") specifies the ways in which EWR collects, handles and stores personal data, and the ways in which employees and other stakeholders protect EWR from the risks of a data breach (as defined below). It further sets out EWR's approach to meeting its obligations under the UK Data Protection Laws.

# 3. Scope and applicability

3.1. This Policy applies to the data of:

a) all EWR employee's data including directors, employees and prospective directors, employees, temporary employees, secondees, contractors, volunteers, and interns, referred to herein as "employees" and "employee-related personal data"; and

b) all EWR's clients, stakeholders and other interested parties including businesses, individuals and elected representatives who have interacted with EWR for business purposes, or other personal data processed for business purposes herein referred to as "clients" and "business-related personal data".

# 4. Objectives

4.1. The Policy aims to:

a) provide a standard (based on the UK Data Protection Laws) for the treatment of personal data across EWR;

b) ensure good personal data handling practices;

c) provide accountability and expectations for those handling personal data;

d) provide information and guidance about how EWR ensures compliance with an individual exercising their rights under the UK Data Protection Laws; and

e) set out the overall data protection framework applicable to EWR.

4.2. Breaches of this Policy may result in EWR disciplinary procedures being invoked against the individuals responsible or involved. These breaches may be treated as gross misconduct and may result in disciplinary sanctions including summary dismissal from EWR. Breaches of this policy may also constitute a criminal act and result in an individual being subject to criminal charges.

4.3. For more complex areas of data protection and privacy laws, these areas are addressed in separate policies and procedures as set out in section 19 – References.

# 5. Corporate Responsibility and Governance

5.1. All EWR employees have a collective responsibility in ensuring EWR's compliance with the UK Data Protection Laws by reading and adhering to this Policy. EWR employees should familiarise themselves with the requirements under this Policy to ensure EWR's compliance with the UK Data Protection Laws. Sanctions for non-compliance under the UK Data Protection Laws are severe; EWR can be subject to a fine of up to £17.5 million or four per cent (4%) of EWR's worldwide turnover (whichever is greater). Questions about this Policy, or requests for further information, should be directed towards the Data Protection Office.

5.2. A Data Protection Officer ("DPO") has been appointed and their role is to:

a) inform and advise EWR and its employees about its obligations to comply with the UK Data Protection Laws;
b) monitor compliance with UK Data Protection Laws, this policy, raising awareness of data protection issues, training staff and conducting internal audits;
c) advise on, and to monitor, data protection impact assessments;
d) cooperate with the ICO on request; and
e) be the first point of contact for the ICO and for individuals whose data is processed (employees, customers etc).

5.3. A "Data Protection Office" function has been established which currently consists of the DPO and their advisor. The Data Protection Office's role is to assist the DPO in performing the duties set out in 5.2 above.

# 6. Processing Personal Data

6.1. **EWR's principles and standards of processing personal data**

In the course of EWR's standard business operations, EWR employees will obtain and process personal data, consisting of candidate-related personal data, employee-related personal data and business-related personal data (for example, personal details including the name and business contact information of employees of service providers and suppliers, as well as land agents and their agents and representatives).

In line with the UK Data Protection Laws, personal data collected and processed by EWR shall be:

a) collected in a fair, lawful and transparent manner;
b) accurate and kept up-to-date. Where personal data is found to be inaccurate or incomplete, EWR will ensure it is rectified;
c) collected for a specified, explicit and legitimate purpose (see section 8 - Lawful Bases of Processing);

d) adequate, relevant and processed only where it is necessary for the purposes for which it is collected;
e) retained for the minimum period required for its purpose, and in accordance with EWR's legal and regulatory obligations (see section 13 - Retention and Disposal of Data);
f) secure and protected including against a personal data breach (see section 14 – Data Protection and Data Security); and
g) safeguarded by comprehensive and proportionate governance measures. This includes this Policy, processing registers and, where appropriate, employee training

6.2. **Processing of special categories of personal data**

The UK Data Protection Laws makes a specific distinction between personal data, special categories of personal data and criminal offence data. Where EWR processes special category data, this is done in accordance with the UK Data Protection Laws (see section 0 - Processing of Special Categories of Personal Data).

# 7. Records of Processing

7.1. EWR maintains records of personal data processing activities for each of its business units in accordance with the UK Data Protection Laws. A processing activity is any business activity, technology, product, service, IT system or application and any other activity which involves processing of personal data.

7.2. The Data Protection Office is responsible for maintaining and updating the records whenever the processing of personal data by EWR changes and reviewing the ROPAs on no less than an annual basis.

# 8. Lawful Basis for Processing

8.1. **EWR's Processing of Personal Data**

Personal data must be processed on the basis of valid legal grounds. Valid legal grounds are given if and to the extent any of the following conditions apply:

a) The consent of the data subject has been obtained;
b) Processing is necessary for EWR to comply with a legal obligation;
c) Processing is necessary for EWR to perform a task carried out in the public interest or in exercise of official authority vested in us;
d) Processing is necessary for EWR to perform or enter into a contract;
e) Processing is necessary for EWR to protect the vital interests of a data subject or another person; or

f) Processing is necessary for the purposes of legitimate interests pursued by EWR or a third party unless there are overriding interests, rights or freedoms of the data subject.

The grounds are recorded in EWR's ROPAs (section **Error! Reference source not found.** – Records of Processing) and EWR's privacy notices (section **Error! Reference source not found.** – Privacy Notices).

If the lawful basis of legitimate interest is identified as the most appropriate for a processing activity, then a legitimate interest assessment must be completed. EWR has a template form of legitimate interest assessment which you may be asked to assist the Data Protection Office to complete. The completed legitimate interest assessment will then be maintained on an ongoing basis by the Data Protection Office.

### 8.2. Data Processing for Marketing Purposes

Should EWR wish to process business-related personal data for marketing and advertising purposes it shall consult with the Data Protection Office before undertaking any such activity.

EWR shall undertake such activity only in accordance with UK Data Protection Laws and the relevant e marketing legislation (currently Privacy and Electronic Communication Regulations). This processing may be based on either express consent (including a request to receive information about a product or deal) or in certain circumstances on legitimate interests,

If an individual objects to the processing of his/her personal data for marketing purposes (either entirely or by a specific channel), EWR will no longer use that individual's personal data for these purposes and will block the relevant personal data accordingly.

### 8.3. Processing of Special Categories of Personal Data

EWR will ensure it has the appropriate valid legal grounds for processing special category data, to the extent any of the processing conditions under the UK Data Protection Laws applies, in particular if:

a) the data subject has given his/her explicit consent, unless we are prohibited by applicable law to rely on such consent;
b) the relevant personal data has been manifestly made public by the data subject;
c) the processing is necessary for EWR to carry out its obligations under employment, social security or social protection law, or a collective agreement; and
d) the processing is necessary for EWR to establish, exercise or defend against legal claims or where courts are acting in their judicial capacity.

EWR must document in its ROPA any processing of special category personal data it undertakes.

### 8.4. Criminal Records Data Processing

EWR will ensure it has the appropriate valid legal grounds for processing criminal records data. EWR acknowledges that a DBS or other similar check which establishes than an individual does not have a criminal record, is considered a criminal record and EWR will document in its ROPA the processing of such criminal record data and the processing condition on which it relies.

# 9. Consent

EWR relies on consent for processing only if there is no other lawful basis on which it can rely.

Section 8.1 sets out the lawful bases on which EWR typically relies for its various specific processing activities.

If personal data is collected using consent, the consenting individuals will generally have increased rights to control the use of their data. These include the right to withdraw their consent (i.e. request that processing is stopped), the right to request erasure of their personal data and the right to a copy of their personal data to be transferred to another third party.

If you are in any doubt as to whether consent or an alternative lawful basis should be applied to your processing of personal data, please speak to the Data Protection Office DPO.

### 9.1. When consent may be required

EWR may rely on consent in order to process business-related personal data to market to clients. Marketing activities include inviting clients to EWR events or sending out EWR publications and e-promos.

EWR also relies on consent in order to process special categories of personal data relating to its employees. For example, to collect special categories of personal data for diversity surveys.

### 9.2. Information to be given when seeking consent

Whenever an individual is being asked for consent, EWR shall notify individuals of:

a) the purpose of the processing activity for which consent is being requested;
b) the data that will be collected and used;
c) the individual's right to withdraw consent (at any time) and how to do this; and
d) the EWR entity (and/or any other parties) that will be involved in processing their personal data as a controller.

### 9.3. How EWR obtains consent

EWR seeks to record consent through requesting an "active opt in" by the individual. Examples of an active opt-in include the individual:

I. ticking an opt in box on paper or electronically;
II. clicking "I accept" or similar;
III. selecting yes/no from equally prominent options;
IV. manually signing a consent statement in paper form; or
V. responding to an email requesting consent.

### 9.4 How EWR withdraws consent

I. EWR ensures that individuals who have given their consent can withdraw their consent as easily as it was given and can withdraw their consent at any time.

II. EWR also requires that consent notices clearly set out the method by which the individual can withdraw their consent. For example, by including a withdrawal link or providing an unsubscribe email address.

### 9.5 Recording and managing consent

#### 9.5.1. Recording consent

EWR shall maintain records of consents obtained, to demonstrate that an individual has provided the relevant consent. If a consent is withdrawn, the individual must be placed on a suppression list for the relevant processing activity (for example, suppression lists for marketing campaigns).

Consent records should include the following details:

I. name of individual who gave consent;
II. date of the consent;
III. details of the consent declaration and the related data subject notice (which will include the information required under section 9.2 - Information to be given when seeking consent);
IV. the form of consent obtained i.e. written, oral, online timestamp etc.; and
V. any withdrawal of consent.

Details should be maintained electronically (such as in an Excel spreadsheet) or electronic consents and details of timestamps. Please refer to the consent record management form for more details.

#### 9.5.2. Active consent management

Consents should be actively managed. This includes monitoring whether a consent has been withdrawn.

Where a data processing activity relies on Consent and the consent is withdrawn, EWR should stop processing that data immediately and records should be updated accordingly.

# 10. Privacy Notices

10.1 **When EWR provides a privacy notice**

10.1.1. EWR shall make the appropriate privacy notice available to individuals where EWR is processing their personal data.

Examples:

I. made available to job applicants before they provide their CVs and/or file their application via an online application tool by including a link in the tool;
II. information to website visitors should be made available when they start using the website;
III. made available to employees by including the information in their employment contract package; and
IV. information is provided to elected representatives, individuals, stakeholders and other interested groups where they interact with EWR in relation to the East West Rail project (see EWR's Website Privacy Notice).

10.1.2. For new processing activities (i.e. additional purposes to those for which EWR originally collected the personal data), EWR shall notify the relevant individuals before any personal data is newly processed. If EWR collects information regularly from an individual for the same purpose, a privacy notice may only need to be given to that individual once. For example, if an employee provides HR with an update of their qualifications and skills on an annual basis, HR will not provide a copy of the applicable privacy notice each time.

10.2. **Current EWR Privacy Notices**

Below is the list of current, live privacy notice (please note that these privacy notices may be updated from time to time, EWR recommends that employees check these privacy notices periodically).

| **Privacy Notice** | **Location** |
|---|---|
| Candidate Privacy notice | IMS ID 2449 – click here |
| Employee Privacy Notice | IMS ID 2452 – click here |

| | |
|---|---|
| Website Privacy Notice (covering website visitors and all other data subjects who are not employees or candidates) | On the EWR website |

# 11. Third Party Service Providers

a) EWR uses third party service providers to process personal data held by EWR.

b) EWR requires that all third-party service suppliers with access to EWR employee-related personal data and business-related personal data:

I. comply with the UK Data Protection Laws;

II. undergo appropriate due diligence to assess their understanding of, and compliance with, EWR's information security and data protection requirements; and

III. enter into a contract with EWR containing appropriate data protection terms. If the third party is considered a processor of EWR, such contract shall meet the requirements of the UK Data Protection Laws. If the third party is a controller of personal data, the contract shall meet the requirements of the ICO's data sharing code of practice.

c) EWR may also require that third party service providers that process high volumes of personal data or special categories of personal data, to undergo regular audits to ensure on-going compliance with EWR's information security standards.

d) Any proposed new contract with a third-party service provider must be approved by the Data Protection Office.

# 12. International Transfers of Personal Data

a) EWR only permits transfers of employee-related personal data or business-related personal data outside of the UK if an adequate level of data protection can be ensured in the recipient country.

b) Where data is accessed from or transferred to countries outside the UK and EEA and whom are not otherwise on a safe list of countries to receive personal data from the EU ("**Non-Adequate Countries**"), EWR will ensure that an appropriate contract is in place and a transfer impact assessment is undertaken to ensure that such transfer of personal data complies with the UK Data Protection Laws.

c) The Data Protection Office must be involved before there is any transfer of personal data to or access of personal data from Non-Adequate Transfers. You should be aware that IT service providers often host data or provide remote support from Non-Adequate Countries and therefore this may not be obvious at first.

d) Any contracts being entered into which relate to the transfer of personal data must be reviewed and approved by the Data Protection Office.

# 13. Retention and Disposal of Data

A key element of managing EWR's risk of data breach and promoting good data management is by ensuring personal data is not retained for longer than is necessary in relation to the purpose for which the data was processed. Please refer to EWR's Retention and Disposal of Data Policy for more information.

# 14. Data Protection and Data Security

14.1 EWR requires that all processing of personal data (including by its third-party service providers) is carried out in a way that ensures the personal data's security and implements EWR's information security requirements.

EWR's security requirements comprise appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access, including, where appropriate, the following types of measure:

a) encryption of the personal data;

b) on-going reviews of security measures;

c) back-up facilities; and

d) regular security testing.

14.2. EWR's suite of data protection and data security policies can be found on the Intranet.

# 15. Data Breaches

In compliance with the UK Data Protection Laws, EWR may be required to notify applicable regulators of any actual or suspected data breach. All employees and third party service providers are required to report data breaches (or suspected data breaches) in accordance with the EWR's Data Breach Policy and Procedure which sets out how data breaches should be managed and resolved.

# 16. Data Subject Rights

You may not provide any information to an individual who is making a data subject request. If you receive a data subject request from an employee or a client, you must immediately notify the Data Protection Office. All employees are required to manage data subject requests in accordance with the EWR's Data Subject Requests Procedure which sets out how Data Subject Requests should be managed.

# 17. Training

All EWR personnel must complete E-learning Annual Training and any other targeted training notified to them from time to time.

# 18. Data Protection Impact Assessments

A DPIA is a process we undertake to help identify and minimise the data protection risks of a project or new processing activity. EWR is required under applicable law to conduct and document a DPIA for certain types of "high risk" data processing activities. The Data Protection Impact Assessment Procedure should be referred to where conducting a DPIA.

# 19. References

19.1 **Applicable and relevant documents**

The following policies and procedures should be read in conjunction with this Policy:

*Table 1 - Applicable and relevant documents*

| Document number | Document title | Version/Revision |
|---|---|---|
| 2450 | Data Subject Request Procedure | See IMS for current version |
| 2448 | Records Management Procedure and Retention Policy | See IMS for current version |
| 2451 | Data Protection Impact Assessment Procedure | See IMS for current version |
| 2453 | Personal Data Breach Policy and Procedure | See IMS for current version |
| 2449 | Candidate Privacy Notice | See IMS for current version |
| 2452 | Employee Privacy Notice | See IMS for current version |

| | | |
|---|---|---|
| TBA | Website Privacy Notice | See IMS for current version |
| EWR-EWR-IT-XX-PY-K-000003 | EWR IT Security Management Procedure | V01 |
| EWR-EWR-IT-XX-PD-K-000003 | EWR IT Usage Policy | V01 |
| EWR-EWR-IT-XX-PD-K-000002 | EWR's Data Procedure | V01 |
| EWR-EWR-IT-XX-PY-K-000002 | EWR Data Policy | V01 |

# 20. Laws and Directives

20.1

*Table 1 - Laws and Directives*

| ID | Legislation/Directive title | Issuing body | Date |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

20.2. **Standards**

*Table 3 - Standards*

| ID | Document number | Document title | Revision |
|---|---|---|---|
| 1 | | | |
| 2 | | | |

# 21. Appendices

*Table 4 - Appendicies*

| | | |
|---|---|---|
| | | |
| | | |