



dbors

DB Rail Solutions

Data Protection and GDPR Policy

Effective May 21st 2025

DB Rail Solutions Ltd
Unit 1 & 2 Ace Business Park,
Burley Close, Chesterfield,
United Kingdom, S40 2WL
Company Number: 16145208

DB Rail Solutions Ltd is registered with the Data Protection Registrar in order to comply with the storage and/or processing of personal information and is also known as the Data Controller. The company will monitor its storage and information processes at frequent intervals in accordance with current legislation and to ensure its continued compliance within the remit of its Data Protection Registration. Any information that is found to be materially incorrect will be amended as soon as practicable or destroyed.

PERSONAL DATA

Personal Data is data consisting of information, which relates to a living individual who can be identified from the information. Personal data includes expressions of opinion about an individual. All personal data must be processed in accordance with the Data Protection Act 2018. The company will ensure that its personnel are aware of their requirement to treat personal data appropriately and where applicable will treat breaches of its requirements under the Data Protection Act seriously, which may include disciplinary action.

In addition, and under the Data Protection Act, the company and others acting on its behalf, will collect, retain and process information about its personnel. The type of information which may be obtained and stored by the company includes [but is not exclusive to] dates of birth, sex, health and the commission or alleged commission of any offences. This information will be used for payroll and personnel management purposes in connection with everyone's contract for services within the company. In addition, the company shall use any data it holds to ensure it can monitor and comply with any current legislation, particularly in terms of equal opportunities and non-discrimination. Where the company holds any employee's or contractors' personal data, it shall check this data from time to time to ensure that it remains accurate. This shall be carried out on a regular basis by contacting each person to confirm the details held on file. Personnel who become aware of a material change to their circumstances, such as their personal details/maiden names/aliases, home address, next of kin or any contact phone numbers; is required to notify the company as soon as practicable.

The company may also collect and store data on any other persons associated with the carrying out of its business, or as part of its recruitment and/or training programme. Wherever possible, any information stored will be verified as correct and will be regularly audited for its accuracy.

DATA SECURITY, CONFIDENTIALITY AND PRIVACY

All data or information sorted or processed on the organisation's systems or transmitted within or from the organisation (e.g. e-mail, voicemail) is the property of the organisation and may be accessed, read or monitored accordingly. Any personnel with access to company IT resources must ensure the confidentiality and appropriate use of any accessible data, by being aware of the security needs of equipment where such information may be held or displayed, as well as the protection of any access rights, such as passwords.

All personnel are required to abide by the privacy rights of all other personnel regarding the disclosure of personal information, as required by current legislation. It should also be noted that disclosure of confidential information to unauthorised persons or entities, or the use of such information for self-interest or advantage, is prohibited as is access to non-public areas of any network drive. Breaches will be treated severely under the company disciplinary rules.

PRIVACY

All users of the company's IT resources are advised to consider the open nature of information disseminated electronically and should not assume any degree of privacy or restricted access to such information. The company strives to provide the highest degree of security when transferring data but cannot be held responsible if these measures are circumvented and information is intercepted, copied, read, forged, destroyed or misused by others.

Though it is not the intention of the company to continuously monitor Internet and e-mail communications, or access data files held by an individual; the company reserves the right to do so at any time. The company has the right to read and/or delete any data stored on company owned or leased equipment. All personnel must be aware that they therefore have no right of privacy in respect to Internet and e-mail communications, or stored data, utilising company owned or leased equipment.

However, it should be noted that the company would not normally access an personnel's data or communications without first requesting permission to do so. Although, in the event of an internal disciplinary investigation, or on the request by a Government Agency, or because of litigation against the individual and/or company, any e-mail or data files may be locked and/or copied to prevent destruction and loss of information. In such cases, the company may revert to its right to view any data held without first requesting the permission of the individual concerned.

Article 5 of the GDPR requires that personal data shall be:

- a. processed lawfully, fairly and in a transparent manner in relation to individuals.
- b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes.
- c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- f. and processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

This Policy is reviewed every 12 months and amended as required.



Dave Barnett
Managing Director
08th January 2025