EUROPEAN UNION AGENCY FOR RAILWAYS

Making the railway system work better for society.

Privacy Notice

Audits & Inspections under Monitoring system for notified conformity assessment bodies

1. Introduction

According to Article 34 of Regulation 2016/796, the Agency implemented a monitoring system to assess notified conformity assessment bodies (NoBos) of the railway sector. The monitoring (audits or inspections) is performed jointly with the Member States' Notifying Authorities, in charge of setting up and carrying out the necessary procedures for the assessment, notification and monitoring of NoBos, ultimately responsible for the assessment of railway products. This Privacy notice outlines the criteria by which the European Union Agency for Railways (ERA) collects and processes personal data in the context of audits and inspections under Monitoring system for notified conformity assessment bodies.

Your personal data is processed in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

Concerning the personal data managed at Member State level, they shall follow the national rules in matters of data protection, in line with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

For more information about the processing in question, you are invited to contact ERA through the addresses provided in section "Contacts".

2. Controller of the processing operation

The Controller determining the purpose and means of the processing of your personal data is the European Union Agency for Railways (ERA). The entity responsible for managing the personal data processing is the Head of Monitoring, Analysis, Research and Stakeholders Unit.

3. Purpose of the processing operation

The information provided along the process is used to:

- perform the monitoring system activity
- assign qualified staff to the monitoring system activity.
- report about the findings to the concerned NoBo, the relevant MS Notifying Authority and to EC.

4. Data Processed

The types of data, including personal data that may be processed, are as follows:

- Personal data (first name, last name, E-mail Address, Company/Organisation name, Professional Address, City, Postal Code, Country, Business Phone Number, Username, assessment role, qualifications)

- Monitoring activity data (audit/inspection outputs such as classified deficiencies or recommendations for improvement)

Appropriate organizational and technical security measures are ensured according to the data protection legislation applicable to EU institutions and bodies.

The Agency's extranet is the preferable means to share documents with the parties involved in the monitoring system.

The EXTRANET working space for the monitoring system is organized in layers with different levels of access; each document is saved in the appropriate layer within the extranet structure.
Access to information stored on EXTRANET is managed via access rights provided to the groups as follows:

- EXTRANET home page accessible to all Agency extranet users;
    - notified CAB monitoring home page to which all the identified groups may access;
        - a sub-page per each Member State (MS), to which only the MS and the Conformity Assessment Body/ies (CAB) established on its territory may access;
            - [if required] a sub-page per each notified CAB established within the Member State to which only the concerned Member State and the CAB itself may access. Sensitive information is stored at this level.

All personal data in electronic format (e-mails, documents, etc.) are stored either on the servers of the Agency's in its premises or alternate site or in Microsoft data centers in the EU (linked to the Agency's and Commission's Office 365 environment).

5. Recipients of personal data are:

The Controller, the Executive Director, ERA staff directly involved in monitoring CABs (namely the responsible for monitoring notified conformity assessment bodies - MNB responsible -, the team leader, technical experts), or supporting functions directly involved in the routine management of the MNB system (such as IT staff or MNB secretariat, the Data Protection Officer, the Legal Officer).

All recipients of the data are reminded of their obligation not to use the data for any further purpose other than the ones for which they were collected.

For services related to the Stakeholder Relations Management Online (SRMO), Microsoft acts as data processor. Microsoft Corporation, as processor, is committed under the terms of the Interinstitutional License Agreement and related documents to respect the obligations of the GDPR.

In compliance with the terms of the Art. 27 of the GDPR, Microsoft Ireland Operations Limited is Microsoft's representative in the European Union Contact details: Microsoft Ireland, South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland.

Transfers of personal data outside the European Union are not foreseen.

However, diagnostic data covered by contractual rules may be sent to Microsoft outside EU territory.

Microsoft commits to have in place written agreements with all sub-processors that are at least as restrictive in terms of data protection and security as their data processing agreement with the EC.

The activities of all sub-processors are in scope of third-party audits.

6. Your Rights as data subject

You have the ***right to access*** your personal data, which is the right to obtain confirmation about your data processed by the Agency and the ***right to ask for correction*** of any inaccurate or incomplete personal data. You have also the ***right to object*** *to the processing or* ***request the removal*** of your personal data, which will be implemented as soon as your specific request will have been deemed legitimate.

If you have any queries concerning the processing of your personal data, you may address them to the data Controller. You will find the address in the Contacts below.

7. Legal basis for the processing operation

Legal basis:

- Article 34 of Regulation (EU) 2016/796 (AR).
- Management Board Decision n°156

Lawfulness:

The processing is lawful under Art. 5.1(a) according to data protection Regulation (EC) 2018/1725: processing is necessary for the performance of a task carried out in the public interest.

8. Time limit for storing the data

Personal information will be retained for a maximum period of 10 years after the conclusion of the assessment-reporting phase.
Regarding the Agency Extranet collaboration space, personal data shall be kept as long as the data subject has access to the Extranet. After the deletion of the data subject's profile, the relevant personal data shall be kept for 13 months and then, will be deleted.

The MNB responsible maintains up to date the membership of the relevant extranet workspace withdrawing undue memberships.

9. Contacts

All your requests concerning your data protection rights should be addressed to the Data Controller at AOD.mars@era.europa.eu.
In case you have any questions related to the protection of your personal data, you can also contact the ERA Data Protection Officer at DataProtectionOfficer@era.europa.eu.
You have at any time the right of recourse to the European Data Protection Supervisor at edps@edps.europa.eu.