

## **Privacy Policy of the Companies of the "Latvijas dzelzceļš" Group**

### **General rules**

1. The purpose of the Privacy Policy is to provide a natural person, such as a customer, party to a contract, authorized representative, contact person, applicant, visitor, participant in a procurement procedure, website user and other persons not listed in this Privacy Policy (hereinafter referred to as the Data Subject), with information on the purpose of processing of personal data, legal basis for processing of personal data, scope and terms of processing of personal data, protection measures implemented by companies of the "Latvijas dzelzceļš" Group (hereinafter referred to as the Group or companies of the Group), as well as the rights of the Data Subject in relation to the processing of personal data of the Data Subject.

2. The Privacy Policy applies to any Data Subject whose personal data are processed by the companies of the Group, regardless by what means and/or in what environment the Data Subject provides the personal data – in person and orally, in writing, by telephone, by electronic mail, on a website or otherwise.

3. Terms used in the Privacy Policy – personal data, processing of personal data, data subject and other terms – are used within the meaning of 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 (hereinafter referred to as the Regulation).

### **Information about Data Controller**

4. When processing personal data of the Data Subject, each company of the Group may be both the data controller and processor or joint controller.

5. Personal data are processed in the Group by the following Group companies:

5.1. SJSC "Latvijas dzelzceļš" – Reg. No.: 40003032065, registered office: Emīlijas Benjamiņas Street 3, Riga; LV-1547;

5.2. "LDZ CARGO" Ltd. – Reg. No. 40003788421, registered office: Dzirnavu Street 147 k-1, Riga, LV-1050;

5.3. "LDZ Loģistika" Ltd. – Reg. No. 40003988480, registered office: Dzirnavu Street 147 k-2, Riga, LV-1050;

5.4. "LDZ ritošā sastāva serviss" Ltd. – Reg. No. Nr.40003788351, registered office: Vilhelma Purvīša Street 21, Riga, LV-1050;

5.5. "LDZ apsardze" Ltd. - Reg. No. 40003620112, registered office: Zasas Street 5-3, Riga, LV – 1057;

5.6. JSC "LatRailNet". – Reg. No. 40103361063, registered office: Pērses Street 8, Riga, LV-1011.

### **Contact details**

6. For the convenience of the Data Subject, companies of the Group have defined one type of contact details/communication in matters related to the processing of personal data and reporting possible personal data breaches: e-mail: [datuaizsardziba@ldz.lv](mailto:datuaizsardziba@ldz.lv). By using this option

or by contacting 3 Gogoļa Street, Riga, inquirers can ask additional questions about the processing of personal data. A request for exercising the Data Subject's rights may be submitted in accordance with the procedures specified in Clause 17 of the Privacy Policy.

### **Purposes of personal data processing**

7. Companies of the Group process individuals' data for the following purposes:

- 7.1. Implementation of external legislation;
- 7.2. Ensuring operations of the companies of the Group;
- 7.3. Ensuring performance of the services of the companies of the Group;
- 7.4. Conclusion and performance of contracts;
- 7.5. Ensuring quality service;
- 7.6. Maintenance of information and technical systems necessary for the provision of services;
- 7.7. Identification of the Data Subject;
- 7.8. Communication with the Data Subject;
- 7.9. Administration of invoices and other financial documents;
- 7.10. Record keeping;
- 7.11. Handling applications/complaints lodged by the Data Subject and other documents;
- 7.12. Prevention and investigation of criminal offences and breaches;
- 7.13. Prevention of fraud;
- 7.14. Collection of the Data Subject's debts;
- 7.15. Provision of information to public administration institutions in the cases and amounts laid down in external legislation.

### **Categories and types of personal data**

8. Companies of the Group mostly process the following categories and types of personal data:

- 8.1. Identification data of the Data Subject – name, surname, personal number, date of birth, passport No./ID number, signature;
- 8.2. Contact details of the Data Subject – address, telephone number, email address;
- 8.3. Data of a cooperation partner's contact persons – person indicated by the cooperation partner who is to be contacted – name, surname, telephone number, email address;
- 8.4. Contract data – contract number, date of signing, contractors, contact details, signature;
- 8.5. Data necessary to ensure the performance of a contract, for example, mandatory data on a product, the customer's freight, its location, etc.;
- 8.6. Data on purchase of a service (goods) – service name, purchase date, invoice number, provision of service, price, payment method, receipt data, service delivery address, etc.;
- 8.7. Data on passengers on the following international rail routes: Riga-Moscow-Riga, Riga-St. Petersburg-Riga, Riga-Minsk-Riga, Riga-Kyiv-Riga;

- 8.8. Archive data at the Railway History Museum and data on persons who access this information;
- 8.9. Location data – for example, data on the destination of a passenger or freight;
- 8.10. Communication data – date of communication, content, status of implementation;
- 8.11. Call transcript data – transcripts, date and time of service phone calls;
- 8.12. Data on payments – current account number, bank account number, invoice number, date, amount, invoice receipt type, payment date, debt amount, debt collection information;
- 8.13. Video data – video data at facilities of the companies of the Group, recording date, time;
- 8.14. Photographs and images – photographs from events at the companies of the Group, date and place of photographs;
- 8.15. Actions performed on the website – visitor's IP address, date, time, duration of the visit, downloaded data, viewed sections, actions performed on the portal;
- 8.16. Professional (employment) data, such as information on education, work experience, current employment, positions, professional activity;
- 8.17. Information about real estate and facilities (real estate, land parcel or building, construction project), for example, address, name, cadastral number, designation, land register data, cadastral data.

#### **Legal basis for processing of personal data**

9. Companies of the Group process personal data of the Data Subject according to the following legal bases:

9.1. For entering into and performing a contract to which the Data Subject is a party or for taking steps at the request of the Data Subject prior to entering into a contract (point (b), paragraph 1, Article 6 of the Regulation), for example, telephone number or email indicated in the contract are used only for communication with the Data Subject;

9.2. For compliance with a legal obligation to which the companies of the Group are subject – compliance with external legislation, for example, in organizing railway services; maintaining the railway infrastructure and ensuring safety on the railway; ensuring that unauthorized persons do not have access to the railway infrastructure and the Group's facilities, thereby ensuring maintenance of public order and safe organization of railway traffic; performing registration and analysis of railway accidents; organizing accounting and record keeping, leasing real estate, etc. (point (c), paragraph 1, Article 6 of the Regulation);

9.3. For the purposes of the legitimate (lawful) interests pursued by the companies of the Group or third parties (point (f), paragraph 1, Article 6 of the Regulation). The legitimate interests of the companies of the Group include, for example:

9.3.1. Conducting a business;

9.3.2. Verifying the identity and legal capacity of the Data Subject prior to entering into a contract or during servicing the Data Subject – by telephone, electronically, in person;

9.3.3. Ensuring implementation of contractual obligations;

9.3.4. Sending messages or otherwise communicating progress of the performance of the contract and developments relevant to the performance of the contract;

9.3.5. Review of the Data Subject's submissions, applications, complaints;

- 9.3.6. Administration of payments and debts;
- 9.3.7. Providing electricity trading services;
- 9.3.8. Providing security services;
- 9.3.9. Providing freight and passenger transport services;
- 9.3.10. Providing services of the Railway Museum;
- 9.3.11. Providing and administering real estate rental and management services;
- 9.3.12. Providing and administering rent of movable property, incl. rolling stock;
- 9.3.13. Providing and administering rent of residential premises;
- 9.3.14. Maintenance of information and technical systems necessary for the provision of services;
- 9.3.15. Ensuring efficiency of services, sale of goods, and shipments;
- 9.3.16. Ensuring and improving quality of services;
- 9.3.17. Training and employment of trainees;
- 9.3.18. Prevention of unfounded financial risks to their business activity (incl. credit risk assessment before the sale of goods and services and during the performance of a contract);
- 9.3.19. Debt collection, protection of the interests of the companies of the Group in court and other state institutions;
- 9.3.20. Prevention of corruption and criminal offenses;
- 9.3.21. Informing the public about the operations of the companies of the Group;
- 9.3.22. Popularizing railway industry at various public events;
- 9.3.23. Analysis of the operation of the websites and Internet sites of the companies of the Group, developing and implementing necessary improvements;
- 9.3.24. Protection of the vital interests of the Data Subject or another natural person, for example, by performing video surveillance (point (d), paragraph 1, Article 6 of the Regulation);
- 9.3.25. In individual cases, also with the Data Subject's consent.

#### **Processing and protection of personal data**

10. Companies of the Group process the Data Subject's data using modern technology, taking into account the existing privacy risks and the organizational, financial and technical resources available to the companies of the Group, and taking at least the following security measures:

- 10.1. Adopt internal policies regarding the protection of the personal data of natural persons;
- 10.2. Confidentiality rules for employees of the Companies of the Group;
- 10.3. Agreements governing the protection of personal data with the contracting parties;
- 10.4. Restricted/controlled access to property and information systems of the companies of the Group;
- 10.5. Educating employees on personal data protection matters;

10.6. Various information technology protection measures are employed, such as firewalls, secure passwords, intrusion protection and detection programs, data encryption mechanisms, etc.

11. The companies of the Group do not use automated decision-making regarding the Data Subject.

#### **Transfer/disclosure of personal data**

12. The companies of the Group do not disclose personal data of the Data Subject to third parties, except:

12.1. To the persons specified in the cases provided for in external legislation, in the procedure and to the extent specified in the external legislation;

12.2. When transferring personal data to a cooperation partner if the data have to be transferred as part of a contract concluded with the relevant cooperation partner for the performance of the contract;

12.3. When the Data Subject has given explicit consent;

12.4. In cases provided in external legislation in order to protect the legitimate (lawful) interests of the companies of the Group.

#### **Access to personal data by third-country entities**

13. The companies of the Group do not transfer personal data to countries outside the European Union and the European Economic Area, except when the companies of the Group transfer personal data to the Russian Federation or the Republic of Belarus, and only if an agreement is concluded with the Data Subject in each individual case, e.g. for performing cargo or passenger transportation in the territory of the Russian Federation or the Republic of Belarus, organized by the companies of the Group.

#### **Period for which personal data are stored**

14. The companies of the Group do not store personal data for longer than is necessary for the purpose of data processing or for longer than required by external legislation. The period for which personal data are stored is determined by various criteria, such as requirements of external legislation, technical capacities for data storage, etc. The companies of the Group store and process personal data of Data Subjects as long as at least one of the following conditions exists:

14.1. As long as stipulated by external legislation, for example, in performing obligations specified in the Law on Accounting and Law on Archives;

14.2. As long as the contract with the Data Subject is in force;

14.3. As long as the companies of the Group pursue their legitimate interests (for example, review of claims, judicial remedy, settlement of disputes, lodging a lawsuit, statute of limitations, etc.);

14.4. Personal data obtained during video surveillance – detailed information is available in the last section of the Privacy Policy;

14.5. Audio recordings of the Data Subject's calls to the Railway Inquiry Service, phone number 1181 and 8001181, are stored for not longer than 13 months.

15. After the circumstances referred to in Clause 14 cease to exist, personal data of the Data Subject are deleted, unless external legislation provides for a different storage period.

### **Rights of the Data Subject**

16. The Data Subject has the right to obtain, according to the relevant legal acts, information regarding the processing of his or her data, including the right to request a company of the Group to access his or her personal data, as well as to request that the data be completed, rectified or deleted, or that the processing be restricted regarding the Data Subject, or object to the processing.

17. The Data Subject may submit a request for exercising his or her rights:

17.1. In writing by visiting a company of the Group in person and presenting identification;

17.2. By electronic mail – by signing the mail with a secure electronic signature and sending it to the following email address: [info@ldz.lv](mailto:info@ldz.lv);

17.3. By sending a written letter to a company of the Group.

18. Upon receiving the Data Subject's request, the company of the Group verifies the Data Subject's identity, assesses the request and complies therewith in accordance with the relevant legal acts. In order for the Data Subject to receive information about him or herself, the company of the Group needs to identify you as the Data Subject, as the companies of the Group cannot provide information to a person without making sure that we provide the information specifically to you. Depending on the situation, the companies of the Group may ask the Data Subject to prove his or her identity with an identification or otherwise.

19. The Data Subject must take into account the working hours of the companies of the Group.

20. The companies of the Group respond to the Data Subject, taking into account the manner of receiving a response indicated by the Data Subject.

21. If the reply is sent by post, it is sent as registered mail, addressed to the person whose personal data have been requested. If the reply is provided electronically, it is signed with a secure electronic signature (if the application has been submitted with a secure electronic signature).

22. The company of the Group ensures the fulfilment of data processing and protection requirements in accordance with the relevant legal acts and, in case of the Data Subject's objection, takes the necessary action to remedy the objection. If this fails, the Data Subject has the right to apply to the supervisory authority – the Data State Inspectorate, 11/13 Blaumaņa Street, Riga.

23. The Data Subject has the right to receive information about his or her personal data processed by the company of the Group, free of charge.

24. Receiving and / or using personal information may be restricted in order to prevent adverse effects on the rights and freedoms of other persons (including employees of the companies of the Group) or in cases where the provision of data is prohibited by external legislation.

25. Where requests for information are manifestly unfounded or excessive, in particular because of their repetitive character, the company of the Group may either: a) charge a reasonable fee based on administrative costs related to the provision of information or communication, or the performance of the requested action, or b) refuse to act on the request.

## **Website visits and cookie processing**

26. The websites of the companies of the Group may use cookies.

27. Cookies are files that websites (hereinafter referred to as the Website) transfer to users' computers in order to identify the user and facilitate the use of the website. Internet browsers can be configured to alert the visitor to the use of cookies and allow the visitor to choose whether he or she agrees to accept them. Not accepting cookies will not prevent a visitor from using the Website, but this may restrict the visitor's ability to use the Website, for example, this may affect certain features of the Website.

Detailed information about cookies used on this webpage can be found on [www.ldz.lv/en/cookie-policy](http://www.ldz.lv/en/cookie-policy) as well as on the website of each company of the Group, as the cookies used may differ from website to website.

## **Information for Data Subjects about video surveillance performed by the companies of the Group**

28. The purpose of video surveillance is to enhance safety and security in the relevant area, including by recording accidents, protection of railway infrastructure objects, enforcing traffic safety on public railways, monitoring access to the Group's buildings and areas adjacent thereto, rolling stock, and ensuring safety and security of facilities, employees and visitors, as well as property of the Group and documents and information stored at the Group's facilities. Certain components of the video surveillance system may be used in investigation of violations of the rules and procedures of the Group. The video surveillance system enables prevention and, if necessary, investigation of public order crimes and security breaches in the area surveyed, reconstruction of the course of events, prevention of potentially dangerous situations or unauthorized physical access, including unauthorized access to enclosed and protected premises and areas, the information technology infrastructure of the Group, as well prevention of theft or physical interference.

29. In order to achieve the purpose of video surveillance, the following conditions are observed: the Group observes the right to privacy and generally accepted ethical norms when performing video surveillance – the video surveillance system covers the immediate vicinity of the Group's buildings, stations, level crossings, railway bridges and other facilities, but not a larger area than necessary for attaining the purpose of the video surveillance system, unless national security interests dictate otherwise.

30. The basis for processing is laid down in points (d) and (e), paragraph 1, Article 6, and point (g), paragraph 2, Article 9 of the 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.

31. Information storage duration – information obtained as a result of video surveillance is stored for up to 2 months, or longer if required by law. At the end of this period, the data are automatically deleted unless the data have been requested or a criminal offense has been identified. If the data have previously been requested by the relevant state or municipal authorities or a criminal offense or violation has been identified, the data are stored as long as necessary.

32. Data protection officer's information: [info@ldz.lv](mailto:info@ldz.lv), telephone 8002 1181.

33. Categories of data processed as a result of video surveillance – video surveillance recordings and images.

34. Recipients or categories of recipients of personal data – Latvijas Dzelzceļš Group transfers data/video material obtained as a result of video surveillance only in the following cases and on the following conditions:

34.1. To pre-trial investigation authorities, bodies performing operational activities, state security institutions, prosecutor's office (for obtaining evidence in criminal cases), courts (for obtaining evidence in pending cases);

34.2. To the capital companies of Latvijas Dzelzceļš Group for attaining the purposes of the processing of data, based on an agreement or the internal regulations of Latvijas Dzelzceļš Group;

34.3. To Data Subjects on the basis of a written application;

34.4. To legal persons on the basis of a valid application or contract.

The procedure for the transfer of video material is regulated by internal regulations and monitored.

35. The data are not transferred to third countries or international organizations.

**36. Rights of the Data Subjects:**

36.1. By submitting a written request, the Data Subject has the right to obtain all information collected about him or her in the video surveillance system, unless disclosure of such information is prohibited by law or the information has already been deleted in accordance with the internal regulations of Latvijas Dzelzceļš Group;

36.2. The Data Subject has the right to receive the above information free of charge, or receive a substantiated refusal to provide information, within one month from the date of submission of the request;

36.3. The Data Subject has the right to rectification and erasure of data, restriction of processing, and data portability;

36.4. The Data Subject has the right to lodge a complaint with the supervisory authority – the Data State Inspectorate, if violations in the processing of personal data have been established.

37. Data Subjects should take into consideration that Latvijas Dzelzceļš Group reserves the right not to release material obtained during video surveillance in cases when such release of data:

37.1. Would affect other data subjects and there would be no technical possibility to provide the information without infringing the rights of other data subjects;

37.2. Would affect provision of information from video surveillance systems at critical infrastructure facilities;

37.3. Requires an excessive amount of time, staff or financial resources due to their size or complexity.

**Information for Data Subjects on the processing of personal data by the companies of the Group during personnel selection**

38. The Group processes individuals' data for the following purposes:

38.1. Selection of personnel for a specific job;

38.2. Selection of personnel for future vacancies;



38.3. To ensure transparency of the personnel selection process and the ability to prove it to the auditors, ensuring availability of facts proving the validity and legality of the decisions taken during the personnel selection process;

38.4. To obtain evidence proving, in case of possible complaints and disputes, the legality of the relevant selection process.

39. The following personal data are processed during the personnel selection process:

39.1. Identification data – name, surname;

39.2. Contact details – email address, telephone number, registered or actual address;

39.3. Information on past work experience;

39.4. Information on the Applicant's qualifications and skills (additional requirements may be set for certain categories of applicants, for example, whether he or she has a driving license, documents certifying proficiency in the state language, etc.);

39.5. Education and training data;

39.6. Other information from the application documents (application letter, CV, certificates, etc.).

40. For each personnel selection competition, the Controller indicates the scope of data to be submitted, the submission of which is mandatory for the Applicant to participate in the personnel selection process.

41. The Group reserves the right to delete personal data received that are not necessary for the evaluation of applications.

42. Legal basis for the processing of personal data and data storage period:

42.1. The legal basis for the processing of personal data by the Group is laid down in point (a), paragraph 1, Article 6 of the Regulation - CONSENT of the applicant, point (f), paragraph 1, Article 6 – legitimate interests of the companies of the Group, and point (c), paragraph 1, Article 6 – legal obligation of the companies of the Group to ensure transparency of the selection process for members of the Management Board and of the Council.

42.2. Consent when applying for a specific position or positions:

42.2.1. When a candidate applies for a specific position or positions in the Group, the companies of the Group receive and use the Applicant's personal data on the basis of the Applicant's consent (consent is provided by the Applicant's actions – submission of application documents to a company of the Group) only for competitions for a specific position or positions that the Applicant has applied for, the data are stored for one year after the vacant position is announced;

42.2.2. The Applicant has the right to revoke his or her consent referred to in this clause at any time by sending a request to [datuaizsardziba@ldz.lv](mailto:datuaizsardziba@ldz.lv). In this case, all personal data submitted by the Applicant on the basis of the specific consent will be deleted;

42.2.3. In the cases referred to in this clause, personal data are stored for one year to enable the Group to protect its legitimate interests and provide evidence in the event of a complaint or a legal dispute to prove the legality of the selection process, as well as to ensure full documentation for the audit to demonstrate transparency of the selection process and validity and legitimacy of the decisions taken. The storage period for the data submitted is reviewed once a year.

43. Consent also for other competitions in the future and for storing the Applicant's data in the Group's database of applicants:

43.1. If an Applicant is not selected for a position in the Group for which he or she applied, but wants the Group to keep the application and the data submitted by the Applicant and use them in other competitions, the Applicant has the opportunity to indicate in the application that he or she wishes to give his or her consent for storage of the data submitted. In this case, the Group may store and use the Applicant's personal data for 1 (one) year from the moment the vacancy is announced. The legal basis for the storage and use of such personal data is the Applicant's consent and the possibility to participate in the Group's future job competitions without announcing the job competitions publicly;

43.2. The Applicant has the right not to give his or her consent referred to in this clause; if consent has been given, it can be revoked at any time by sending a request to [datuaizsardziba@ldz.lv](mailto:datuaizsardziba@ldz.lv). In this case, all personal data submitted by the Applicant on the basis of the specific consent will be deleted;

43.3. In the cases referred to in this clause, personal data are stored until the given consent is revoked or for 1 year from the moment the vacancy is announced so that the Group can use the personal data for other competitions or vacancies.

44. Submission of other personal data.

44.1. The Applicant has the right to submit to the Group personal data of other persons only in exceptional cases, for example, by submitting personal data of a person who gives or could give a reference for the Applicant's past work experience. In such cases the Applicant, as a controller, is responsible for complying with the legal basis for submitting these personal data to the Group and other applicable requirements. The Group always reserves the right not to accept personal data it has not requested.

#### **Other provisions**

45. The Privacy Policy may be amended and extended, and such amendments and extensions are made available to the Data Subject by posting relevant information on the websites of the companies of the Group.

46. The companies of the Group keep the previous versions of the Privacy Policy and they are available on the websites of the companies of the Group.

Security Director

A.Grigulis