



---

## Freeport of Riga Authority PRIVACY POLICY Contents

1. General information
2. The Freeport of Riga Authority details and contact information
3. Purpose of personal data processing
4. Lawfulness of personal data processing
5. Processing of special categories of personal data
6. Website visits and cookie handling
7. Personal data recipients
8. Personal data retention period
9. Data protection
10. Your rights

### 1. General information

The Freeport of Riga Authority (hereinafter - "FPRA" or "we") is a derived public person that ensures the management of the Freeport of Riga, operating in the field of public and private law. It operates under the supervision of the Cabinet of Ministers. The Freeport of Riga is a multifunctional, modern and long-term-development-oriented port at the crossroads of transport corridors with an increasing role in the global and regional transport chain and the passenger traffic network of the Baltic Sea region. The FPRA respects your privacy and undertakes to protect it in accordance with the present privacy policy (hereinafter - the Privacy Policy). The objective of the present Privacy Policy is to provide you with information about the purpose for which we collect personal data, about the amounts of data and deadlines for data processing, about data protection, as well as to inform you about your rights and obligations.

Personal data is any information relating to an identified or identifiable natural person (data subject). Personal data include any information by which a person can be identified, directly or indirectly, such as name, last name, personal identification number, residential address or actual location, as well as physical, physiological, genetic, mental, economic, cultural or social identity factors of that person and other similar information which characterizes that person and enables him or her to be identified, directly or indirectly. With regard to your personal data, we are the data controller who determines the purposes and means of the personal data processing.

When processing personal data, the FPRA observes laws and regulations in force in the Republic of Latvia, the General Data Protection Regulation (hereinafter - the Regulation), as well as other laws and regulations in the field of privacy and personal data processing.

The Privacy Policy applies to any natural person whose personal data is processed by FPRA and shall apply



to the processing of personal data, regardless of the form in which you or any other natural person submits personal data to us – either electronically, on paper or by telephone.

The present version of the Privacy Policy is effective as of February 17, 2020. The FPRA is entitled to introduce amendments and additions to it. The current version of the Privacy Policy is published on the FPRA website. The Privacy Policy in paper format is available at the FPRA legal address.

## **2. The FPRA details and contact information**

The FPRA has the following taxpayer code: 90000512408. The legal address of the FPRA is 12, Kalpaka boulevard, Riga, LV-1010; phone: 67030800; electronic mail address: [info@rop.lv](mailto:info@rop.lv); website address: [www.rop.lv](http://www.rop.lv). To contact the FPRA data protection specialist, please write to the e-mail address [pdapstrade@gmail.com](mailto:pdapstrade@gmail.com).

## **3. Purpose of personal data processing**

We process personal data for the following purposes (objectives):

Providing cooperation with merchants operating in the FPRA territory. This objective includes all activities that are necessary for the FPRA to be able to implement its basic function in relation to the management of the Freeport of Riga territory and the development of commercial activities in the said territory. In order to achieve this objective, we process the personal data of the members of the Council and the Board of the merchants and representatives of the merchants to the extent necessary.

Acquisition of goods and services required by the FPRA, as well as performance of agreements/contracts, concluded with the FPRA, and services provided by the FPRA. For this purpose, we process the personal data necessary for the conclusion and performance of the contract/agreement, the provision of services, the administration of settlements, the debt recovery and collection, the submission, review and processing of claims, and similar purposes.

Staff recruitment. We process the data of persons who have expressed a wish to apply for vacancies at the FPRA. The data obtained in the employee recruitment process are used only to assess the applicant's eligibility for the position. We do not request data that does not relate to the performance of the intended work or is not related to the applicant's suitability for the position. We also do not request information that is not necessary for the assessment of eligibility for the position, and we do we comply with the restrictions set forth in the Labor Law regarding the request for information. We obtain feedback from previous jobs only on condition that the applicant has given prior written consent. Applicants' personal data is processed in compliance with the terms and conditions set out in the present Policy. We process the personal data of our employees in compliance with the requirements of the Labor Law and other laws and regulations.

Accounting and record keeping. The FPRA maintains accounts in accordance with the requirements of laws and regulations. Within the said framework, personal data is processed in the necessary amount and in accordance with the procedures specified in laws and regulations. We also process personal data with the aim to provide for the FPRA incoming and outgoing correspondence, to process applications/ requests and



respond to them, issue references, ensure correspondence, and handle other matters related to record keeping.

Video surveillance. For security, surveillance and property protection purposes, video surveillance is performed at the FPRA objects and territory. Video surveillance recordings are stored for a maximum of 3 months. After expiration of the said period, we delete these recordings, unless the video surveillance recordings have been previously requested by the competent state or local authorities, or criminal offenses have been identified. In this case, the retention time of the video recordings is determined according to the need.

Ensuring control of the access to the objects under the responsibility of the FPRA. According to applicable laws and regulations the FPRA is obliged to organize and take measures to ensure the protection of the port, berths, terminals and the territory. Among other things, the port territory is subject to a special pass and security regime. The procedure for receiving passes is stipulated by the FPRA Regulations “On the Pass Regime in the Freeport of Riga”. In order to enter the territory of the Freeport of Riga, it is necessary to receive a pass issued by the Port Police. To receive a pass, it is necessary to submit the following personal data: name, last name, personal identification number (if there is no personal identification number, then a person’s ID or date of birth, and identity document data), position, e-mail address, telephone number. If the site is visited by a vehicle, the make of the vehicle and national registration number shall be provided. It is not possible to obtain a pass without submitting these data. Road freight carriers shall present an identity document and a registration certificate of the vehicle and its trailer upon entering and leaving the territory of the Freeport of Riga.

Drawing protocols of administrative violations detected in the territory of the Freeport of Riga. If an administrative violation is identified in the territory of the Freeport of Riga, the Port Police draws up an administrative violation protocol, processing the following personal data: name, last name, personal identification number, place of residence, data of personal identification documents, and information on the violation.

Making voice recordings when communicating with vessels. We record radio communication with ships entering and leaving the Freeport of Riga, as required by the International Ship and Port Facility Security Code.

Exemption of the Master from the obligation to use the services of a pilot. This purpose of personal data processing includes the processing of personal data, which is necessary in order to issue a permit to the Master of the ship to navigate in the port water area without using pilotage services in the cases provided for in laws and regulations. The processing of personal data is performed only after the receipt of a person’s application for the issuance of such a permit. The following data are processed for this purpose: name, last name, personal identification number, position, information on education, qualifications and experience.

Requests. Upon receipt of a relevant request, we provide information to public institutions and subjects of operational activities in the cases and to the extent specified in laws and regulations.

Other cases. We process personal data in unspecified, special cases, informing the data subject of the purpose of the processing before obtaining the data, as well as in exceptional cases, in order to protect the



vital interests of the data subject or a third party.

#### **4. Lawfulness of personal data processing**

The FPRA processes personal data only for lawful purposes, i.e. if at least one of the following reasons can be established:

- the processing of personal data is necessary for the performance of a contract to which the data subject is party or in order to take action at the request of the data subject prior to the conclusion of the contract
- the processing is necessary for the protection of our or a third party's legitimate interests, unless the interests of the data subject or the fundamental rights and freedoms requiring the protection of personal data outweigh such interests, in particular where the data subject is a child;
- the data subject has consented to the processing of his or her personal data for one or more specific purposes;
- the processing is necessary for compliance with a legal obligation applicable to the FPRA;
- the processing is necessary in order to protect the vital interests of the data subject or of another natural person.

The FPRA does not implement automated decision-making, including profiling.

#### **5. Processing of special categories of personal data**

Special categories of personal data are data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic data, biometric data for the unique identification of a natural person, health data or data on a person's sexual life or sexual orientation. As a data controller, we do not process specific category data of data subjects. The only exception can be made if required by law (e.g. the results of medical examinations of employees are being processed) or the said data is processed at the initiative of the data subject, or if the processing is necessary to protect the data subject's vital interests (e.g. due to sudden deterioration of the data subject's health, it is necessary to call an ambulance, and in similar emergencies).

#### **6. Website visits and cookie handling**

The FPRA website uses cookies. Cookies are small alphanumeric files that we store in your browser or on your device's hard drive. There are different types of cookies that we use for different purposes; but in general, cookies help us to distinguish you from other users of the website. This helps us to make our website easier to use for our visitors as well as to introduce improvements. You can block the use of cookies at any time by activating your browser settings, which enables you to refuse the use of some or all cookies. Our website may contain links to third party websites. These third parties have their own privacy policies that are in no way related to the FPRA. The FPRA is not responsible for the terms of use of these websites and their privacy policy.

#### **7. Recipients of personal data**

We transfer your data to the persons provided for in external laws and regulations in the order and to the



extent provided by the relevant law or regulation (for example, to the State Revenue Service, law enforcement authorities, etc.). We may also transfer your data to third parties in cases provided for by laws and regulations for the protection of our legitimate interests (for example, by bringing a claim to court in regards of the concluded contract performance, debt collection, etc.).

We use the services provided by third parties, which help us to fulfill our obligations under laws and regulations and to manage our operations. These are third parties such as credit institutions in connection with the settlements to be made; our information technology, software and database providers and their maintenance and administration services; cloud computing service providers; providers of legal, accounting and auditing services; debt collection companies; document copying, scanning and destruction service providers; third parties, which provide sending notifications and information; third parties, which provide for events organized by the FPRA, etc.

In each specific case, we provide the data processor with the amount of your data that is necessary for the respective purpose and task. Data is processed only for this purpose and task; it is protected in accordance with the requirements of the Regulation and other applicable laws and regulations.

## **8. Personal data retention period**

The FPRA stores your data for no longer than is necessary for the purposes of its processing. Data is stored as long as:

- the agreement or contract concluded between us is valid, and as long as one of the parties to the agreement or contract can implement its legitimate interests (for example, to submit claims and applications, to bring a claim before a court, etc.);
- the processing of data is necessary for us to be able to fulfill legal obligations applicable to us;
- the processing is necessary to protect your or a third party's vital interests;
- your consent to the relevant processing of personal data is valid, unless there is another lawful basis for the processing of personal data.

Once the above conditions have ended, your personal data will be permanently deleted.

## **9. Data protection**

The FPRA has taken the necessary measures to ensure adequate protection of personal data. We use a variety of security technologies and procedures to protect your personal data from unauthorized access, use or disclosure. However, with regard to the data transmission via the Internet, please note that absolute security cannot be guaranteed for any data transfer over the Internet. Please assess on a case-by-case basis the risks associated with the information confidentiality that you will have to bear if you decide to transfer any personal data to us via the Internet.

## **10. Your rights**

The Regulation provides a number of rights that you can exercise at any time by contacting us. We undertake to provide you with the opportunity to exercise these rights and fulfill your obligations under the



Regulation and other laws and regulations.

You have the right to receive confirmation from us as to whether or not your data is being processed and, if so, to access and receive the following information about your data: the purposes of the processing; categories of personal data; the recipients or categories of recipients of the personal data to whom the data are or will be disclosed; retention period of personal data or the criteria according to which the retention period is determined; that there is a right to request the rectification or erasure of personal data or a restriction on the processing or the right to object to such processing; all available information about the data source, if the data has not been received from you; information on guarantees regarding data processing if the data are transferred to a third country or an international organization.

You have the right to ask us to correct your data if it is inaccurate.

You have the right to request the deletion of your data, and we will comply with this request without delay if at least one of the following conditions is met:

- the data are no longer necessary for the purposes for which they were collected or otherwise processed;
- you withdraw your consent to the processing of data and if there is no other legal basis for their processing;
- if the processing is justified by the legitimate interests of us or a third party, there is no overriding legitimate basis for the processing;
- you object to the processing of your data for direct marketing purposes;
- if the data have been processed unlawfully;
- to ensure the fulfillment of a legal obligation specified for us in laws and regulations;
- if your data were collected in connection with the provision of information society services.

You have the right to request that we restrict the processing of your data. We will comply with this request without delay if at least one of the following conditions exists:

- if you dispute the accuracy of the data - for a period of time during which we can verify the accuracy of your data;
- if the processing is unlawful, but you object to the deletion of the data and instead request a restriction on the use of the data;
- we no longer need your data, but you need it to establish, exercise or defend legal claims;
- you have objected to the processing of your data based on the legitimate interests of us or a third party until it has been verified that our legitimate reasons outweigh your legitimate reasons.

You have the right, at any time, to object to the processing of your personal data based on our legitimate interests or that of a third party, based on reasons relating to your specific situation. In this case, we will no longer process your data, unless we indicate compelling legitimate reasons for processing that are more important than the interests, rights and freedoms of the data subject, or for establishing, exercising or defending legal claims.

If you believe that your personal data is being processed unlawfully, unreasonably, or that their processing otherwise violates the requirements of the Regulation or other laws and regulations, or you have any doubts or questions about the processing of your personal data, please do not hesitate to contact us, submitting a relevant application or complaint. We will provide answers to all your questions and correct mistakes, if any.



---

If you believe that your personal data is being processed unlawfully, unreasonably, or that their processing otherwise violates the requirements of the Regulation or other laws and regulations, you have the right to submit a complaint to the Data State Inspectorate.