PROCEDURE
ON PROCESSING OF PERSONAL DATA

RBGL-RBR-PRC-Z-00004

Revision Number:	1.0	**Effective From:**	2024-08-07

Document owner	Head of Legal Department	Raivo Raudzeps
Prepared by	Lawyer	Andris Vējiņš
Reviewed by	Head of IT Department	Ģirts Dravenieks
	Head of Security Department	Māris Dzelme
	Acting Head of HRM and Administration Department	Agate Pitkeviča

Approved by	Management Board Member	Kitija Gruškevica

THIS DOCUMENT IS REVIEWED AND APPROVED ELECTRONICALLY IN EDMS

DOCUMENT UNCONTROLLED WHEN PRINTED

Co-funded by
the European Union

DOCUMENT HISTORY

This document has been issued and amended as follows:

Revision	Effective from	Author	Description of changes
1.0	2024-08-07	Andris Vējiņš	First issue

CONTENTS

ACRONYMS AND ABBREVIATIONS

A full list of acronyms and abbreviations can be found in RBR Glossary of Abbreviations. The following acronyms and abbreviations are used throughout this document:

Abbreviation	Definition
DPIA	Data Protection Impact Assessment according to Article 35 of the GDPR.
DPO	Data protection officer (either internal or outsourced), but if there is no such person – the Head of Legal Department or his / her nominated person from the Legal Department.
GDPR	Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
IT	Information technologies.
RBR	RB Rail AS, Reg. No 40103845025, a joint stock company registered at the Enterprise Register of the Republic of Latvia, including its Branches (in Estonia, Latvia and Lithuania).

DEFINITIONS

The following terms are used throughout this document:

Term	Definition
Authority	The respective governmental supervisory authority in accordance with the GDPR.
Branches	RBR branch in Estonian (RB Rail AS Eesti filial, registration number: 14168654), RBR branch in Lithuanian (RB Rail AS Lietuvos filialas, registration number: 304430116), RBR Branch in Latvia (RB Rail AS Filiāle, registration number: 40203254781).
Breach	A breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Personal data transmitted, stored or otherwise processed by the RBR.
Breach Register	A register of Breaches.
Classified Information	Documented information which is classified as Limited Access Information or Restricted Access Information.
Controller	The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal data; where the purposes and means of such Processing are determined by European Union or European Union member state law, the controller or the specific criteria for its nomination may be provided for by European Union or European Union member state law.
Consent	Any freely given, specific, informed and unambiguous indication of the Data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Criminal Convictions and Offences data	Personal data relating to criminal convictions and offences or related security measures.

Data subject	Any identified or identifiable natural person (inter alia, including the Employees or the employees of any third parties) who may be identified using the Personal data.
Document	A set of information or data that has been drawn up in paper, electronic or audiovisual format (inter alia, tables, maps, plans, reports, studies, sketches photographs and other objects) by the RBR, a subject of public or private law or a natural person for the purpose of initiating, continuing, altering or terminating an action and which attests this action.
Employee	Any employee of the RBR, including employees of Branches, as well heads/directors of Branches, the Management Board members and the Supervisory Board members of the RBR. For the purposes of this procedure, the trainee is also considered an Employee.
Human Resources Department	The HRM and Administration Department of the RBR.
Generally accessible information	Information other than Classified Information available to Employees without any restrictions imposed and may be publicly available, if it is not for internal use only.
Global Project	Rail Baltica Global Project.
IT Department	IT Department of the RBR.
Information for internal use only	Generally accessible information that due to its nature can't be made publicly available without previous authorization of the information owner and is intended for internal use in RBR only. When necessary, information might be made available to other Global Project organizations and stakeholders but not to general public.
IS or Information system	Complex of software and hardware systems that support data-intensive applications and focuses closely on information handling processes.
Legal Department	Legal Department of the RBR.
Limited Access Information	Information of limited accessibility intended for a limited number of persons for the purpose of fulfilling the assigned professional duties and tasks and disclosure or loss whereof due to the nature or content of such information impedes or could impede the functioning of the RBR, related companies thereof or another institution involved in the fulfilment of the tasks of Global Project or/and state administration, becomes detrimental or could become detrimental to the legitimate interests of persons.
Management Board	The management board of the RBR.
Personal data	Any information relating to the Data subject from which the Data subject can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of the Data subject. Personal data includes both the objective data (e.g., person's name, surname, personal identification number, phone number, address etc.) as well as subjective data (e.g., information included in evaluation forms); irrespective of its form, i.e., it might be stored as a printout, electronic, photographic, audio or video recording.
Procedure	This Procedure on Processing of Personal Data.
Processing (to Process)	Any operation or set of operations which is performed on Personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction, etc.

Process owners	A separate department of RBR or an identifiable Employee or other persons responsible for specific process that includes Processing of the Personal data. Where the department of RBR is deemed to be the Process owner, the head of the respective department shall be responsible for ensuring that the requirements of this Procedure are complied with. For example - to conclude an employment contract with new employees, it is necessary to process employees' data (name, ID number, etc.). The Process owner of this process is Human Resources Department. All Process owners must be registered in Processing Register.
Processing Register	The data base containing info on Processing activities that allows to make an inventory of the Processing activities and have an overview of what RBR is doing with Personal data. It is made according to Article 30 of the GDPR. The Processing Register is formed as a separate Internal Governance Document (document number: RBCR-RBR-XX-XX-REG-Z-00001).
Processor	A natural or legal person, public authority, agency, or other body which Processes personal data on behalf of the RBR.
Procurement Department	The Procurement Department of the RBR.
Pseudonymisation	The Processing of the Personal data in such a manner that the Personal data can no longer be attributed to a specific Data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal data are not attributed to an identified or identifiable natural person.
Restricted Access Information	Information of restricted accessibility in the field of national security (such information applies to military, political, economic, scientific, technical, intelligence (counterintelligence) and operational activity and does not contain a state secret).
Security Department	The Security Department of the RBR.
Special Category Personal data	Personal data that reveal the Data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, or biometric data (if it is used for the purpose of uniquely identifying a natural person), data concerning health or data concerning the Data subject's sex life or sexual orientation.
Supervisory Board	The supervisory board of RBR.

1. OBJECTIVE

1.1. The purpose of this Procedure is to:

1.1.1. inform Employees of the requirements related to the Processing of the Personal Data;

1.1.2. define the organisational measures and necessary technical means, which ensure that rights of the Data subject are respected;

1.1.3. ensure that RBR Personal data Processing protection system is secure and complies with applicable laws.

2. SCOPE

2.1. The Procedure shall be binding to all Employees who, when carrying out their direct work or other tasks, handle the Personal Data at the disposal of the RBR. It must also be ensured that any third parties (i.e., Processors) involved in the protection or the Processing of the Personal data on behalf of the RBR comply with the requirements of this Procedure as far as reasonably practicable.

3. GENERAL INFORMATION

3.1. The reason for this Procedure is that the RBR has to comply with the requirements that have been introduced the GDPR and Personal Data Processing Laws.

3.2. Unless otherwise stated in the Procedure, the Legal Department and/or the DPO is responsible for supervising the protection of the Personal data at the RBR as well as controlling the conformity of the Processing of the Personal data with the requirements of the applicable laws. The Legal Department shall identify the possibility of threats to Personal data processed, as well as advise other RBR's departments on how the Processing should be conducted.

3.3. Within the scope of its competence (to the extent defined in internal procedures), the IT Department and the Security Department is responsible for ensuring compliance of the RBR's IT and IS resources with the requirements of the applicable laws and RBR's internal procedures (including this Procedure).

3.4. When a general reference to the RBR is made in the Procedure, the respective activity must be performed by the Employee who is required to carry out such activity or an activity of a similar nature under an employment contract or other procedures issued by the RBR. In case of doubt, the Legal Department should be involved, and the Legal Department's instructions must be followed.

4. GENERAL PROCESSING RELATED PRINCIPLES AND LEGAL GROUNDS

4.1 PROCESSING RELATED PRINCIPLES

4.1.1. Personal data Processing must always be in line with all the following principles:

4.1.1.1. Lawful basis: for the Processing to be lawful, specific grounds for the processing ('lawful basis') must be identified prior the Processing. In general there are six (6) main lawful basis (see Clause 4.2.1 of the Procedure) with separate lawful basis when it comes to the Processing of Special Category Personal data or Criminal Convictions and Offences data (see Clause 4.2.2 and 4.2.3 of the Procedure).

4.1.1.2. Fairness: it means that the Processing must be done in ways that Data subject could reasonably expect and not in ways that have unjustified adverse effects on them. Assessing whether the Processing is fair depends mainly on how the Personal data was obtained and how the Processing affects individuals, therefore this aspect must be evaluated each time individually (it is not possible to carry out a single assessment valid for all the Processing operations).

4.1.1.3. Transparent Processing: it means an obligation of being clear, open, and honest with Data subjects from the start, for example, by telling what the RBR is and how the RBR shall Process their Personal data. Informing Data subjects in easily accessible form and understandable language is the key.

4.1.1.4. Purpose limitation: Personal data must be collected for specified, explicit and legitimate purposes and may not be further Processed in a manner that is incompatible with those purposes. The specific purpose must be defined before Personal data collection. The Processing for a purpose other than that for which the Personal data have been collected is only permitted in exceptional cases when the applicable laws permit the Processing for another compatible purpose or if it is based on the new Consent or this kind of necessity arises out of legal requirements or priorly evaluated legitimate interests of the RBR.

4.1.1.5. Data minimization: the Personal data may only be collected and otherwise Processed to the extent absolutely necessary to fulfil the defined purpose. The Processing must be adequate, relevant, and limited to what is necessary in relation to the purposes for which the Personal data is Processed. The RBR should never have more Personal data than what it needs to achieve the predefined purposes of Processing;

4.1.1.6. Accuracy: reasonable steps must be taken, including by person processing the Personal data, to ensure that the Personal data that are inaccurate, having regard to the purposes for which they are Processed, are erased or updated without undue delay.

4.1.1.7. Storage limitation: the Personal data must be kept in a form which permits identification of the Data subjects for no longer than is necessary for the purposes for which the Personal data are Processed or due to other legal requirements (particularly to comply with statutory retention periods). After this point, unless specific exception applies, the Personal data must generally be erased or Pseudonymised. In order to determine retention periods, person that Processes Personal data must consider several factors including to what extent it is needed to keep a record of a relationship with the Data subject once that relationship ends, to what extent it is necessary to keep the Personal data to defend from possible future legal claims, to ensure compliance with industry standards and guidelines, and any legal or regulatory requirements.

4.1.1.8. Integrity and confidentiality: the Personal data must be Processed in a manner that ensures appropriate security of the Personal data, including protection against unauthorized or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures. Criterion of sensitivity of Personal data and the risks posed by the Processing operations must be taken into account when particular security measures are selected;

4.1.1.9. Personal data are not transferred to third parties without appropriate precaution: there must be a legal basis and precautionary measures in place in order to transfer Personal data to third parties (especially when transfer of the Personal data includes the transfer of Personal data to countries that are not the European Union member states since in such cases requirement

set out in Chapter V "Transfers of personal data to third countries or international organisations" of the GDPR must be met).

4.1.1.10. Personal data are Processed in compliance with the Data subject's rights: Data subjects have the right to access their Personal data, stop them from being used if the Processing is causing excessive distress to the interests or fundamental rights and freedoms of the Data subject which require protection of personal data, prevent them from being used for direct marketing, have inaccurate Personal data rectified, claim compensation for damaging data breaches and other right mentioned in the GDPR and this Procedure. In certain cases, Data subjects have the right to request that specific Personal data are deleted.

4.1.1.11. Accountability: Employees and other authorized personnel who Process Personal data must ensure that all the above-mentioned principles are taken into account and should be able to demonstrate the compliance with them.

4.1.2. The Special Category Personal data are especially sensitive and therefore a high degree of protection must be applied. Unless applicable laws stipulate otherwise, the Special Category Personal data should only be Processed in exceptional cases. The Special Category Personal data should be separated from other data and access to such data should be limited and enhanced security requirements should be set for working with such data. Any new type of Processing of the Special Category Personal data must always be consulted with the Legal Department and/or DPO prior to such Processing.

4.1.3. Within the RBR, only employees of Legal Department, Security Department, or Procurement Department (procurement commission on procurement related matters) are authorised to Process Criminal Convictions and Offences data. It is not permissible that other Employees are involved in the processing of such data, for example, as intermediaries in transfer operations. If Criminal Convictions and Offences data are to be obtained from business partners or potential employees, such persons should be asked to send these types of Personal data directly to the Employee whose duties include the Processing of such Personal data.

4.2 LEGAL GROUNDS FOR LAWFUL PROCESSING OF THE PERSONAL DATA

4.2.1. Unless the exceptions referred to in Clauses 4.2.2 and 4.2.3 of this Procedure apply, the Processing of the Personal data is lawful only if and to the extent that at least one of the following applies:

4.2.1.1. the Data subject has given the Consent to the Processing of their Personal data for one or more specific purposes. Any element of pressure or inappropriate influence which could affect the outcome of the Data subject's choice to provide the Consent renders the Consent invalid;

4.2.1.2. the Processing is necessary for the performance of a contract to which the Data subject is party or in order to take steps at the request of the Data subject prior to entering into a contract;

4.2.1.3. the Processing is necessary for compliance with a legal obligation to which the RBR as the Controller is subject: If the RBR has a legal duty for which particular Personal data need to be Processed (Processing must be done according to applicable laws and there is no option not to do that), this legal ground should be used;

4.2.1.4. the Processing is necessary in order to protect the vital interests (e.g., essential for the life and/or health related matters) of the Data subject or of another natural person;

4.2.1.5. the Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the RBR as the Controller;

4.2.1.6. the Processing is necessary for the purposes of the legitimate interests pursued by the RBR as the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data subject which require protection of the Personal data, in particular where the Data subject is a child: this legal ground can be used in situations when the interests, rights or freedoms of the affected Data subjects do not override the RBR's interests. To compare these potentially opposing sets of interests, 'balancing test' must be conducted (the RBR's interests must be balanced against the Data subject's interests). If Data subjects would not reasonably expect the Processing, or if it would cause unjustified harm, their interests are likely to override the RBR's legitimate interests and Processing can't be based on this legal ground.

4.2.2. The Processing of the Special Category Personal data is lawful if and to the extent that at least one of the following applies:

4.2.2.1. the Data subject has given explicit consent to the Processing of their Personal data for one or more specified purposes, if obtaining of such consent is not prohibited by the applicable laws;

4.2.2.2. the Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law the processing of those personal data for one or more specified purposes;

4.2.2.3. the Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

or in case there are other, very specific legal grounds that are mentioned in the Article 9 Paragraph 2 of the GDPR.

4.2.3. The Criminal Convictions and Offences data within RBR may be Processed only in exceptional cases when the Processing is authorised by applicable laws (for example, Public Procurement Law of the Republic of Latvia).

5. PERSONAL DATA PROCESSING AT THE RBR

5.1 GENERAL PROCESSING RELATED REQUIREMENTS

5.1.1. Unless required otherwise by applicable laws, ultimately the Processing of the Personal data will only be carried out to achieve goals (purposes) which are necessary to successfully finish Global Project. When Processing of the Personal data, it is always necessary to comply with the principles set out in Paragraph 4.1. "PROCESSING RELATED PRINCIPLES" of this Procedure and to ensure that the Processing is only carried out when a specific legal ground, indicated in Paragraph 4.2 "LEGAL GROUNDS FOR LAWFUL PROCESSING OF THE PERSONAL DATA" has been identified.

5.1.2. The RBR establishes and maintains Processing Register which shall be regularly reviewed and updated in accordance with factual Personal data Processing. Preparation of such Processing Register is a responsibility of the Legal Department.

5.1.3. If the Personal data is to be transferred to any third party a review must first take place in order to determine whether contractual agreements regarding data protection and privacy are needed and, if needed, are in place (see Paragraph 5.7 "INVOLVEMENT OF THE PROCESSORS" of this Procedure). Also, in cases when transferring Personal data to a third party (especially to independent Controllers), the RBR must make sure that there is a legal ground for such Processing activity and that the principles of Personal data Processing are also respected in this case.

5.1.4. Where large amounts of Personal data (not usual for regular business activities, for example, database or part of database) or Special Category Personal data are disclosed to third parties, the RBR (in person of a designated representative from Legal Department) records data related to Personal data disclosure time; person disclosing the information; person requesting and receiving information; amount of disclosed information in the Processing Register. In such cases a prior approval from Legal Department must be obtained. Despite the above, even when a minimal amount of Personal data is disclosed to third parties, it is always highly recommended to keep in writing in a single register the information relating to the time of the disclosure of Personal data; the person who disclosed them; the amount of the disclosed Personal data.

5.1.5. The RBR ensures that Personal data collection, recording, sorting, storing, copying, rewriting, modifying, editing, deleting, destroying, archiving, backup copying, blocking etc., is performed only by authorised personnel (authorisation may be based on an employment contract, an authorisation agreement, power of attorney and other documents obliging or authorising the performance of the act in question) and/or Personal data Processor, as well as provide ability to ascertain Personal data which were Processed without relevant authorisation, in addition to time and person, which Processed Personal data.

5.2 SECURITY RELATED MEASURES

5.2.1. The RBR must implement and continue to take appropriate technical and organisational measures to ensure the protection of the Personal data against misuse, accidental or unlawful destruction, alteration, unauthorized disclosure or access loss and damage, and to treat the Personal data in accordance with the GDPR and other applicable laws. Enhanced protection against unauthorised Processing must be provided for Special Category Personal data and Criminal Conviction and Offences data. Regardless of the type of Personal data, where databases are created and in other case where it is reasonably possible, 'encryption at rest' and 'encryption in transit' principles must be implemented. If specific security measures are applicable to any of the Processing operations, this must be indicated in the Processing Register and Process owner must take all the necessary steps to ensure that this is complied with.

5.2.2. The Processing of the Personal data must be performed on the RBR's premises, Processor's premises (according to written service agreement, which is signed prior to Personal data Processing) or in other location adhering to the RBR needs and instructions (internal laws and regulations). As far as reasonably possible, Personal data must be processed digitally by using the RBR's IT infrastructure and/or RBR used services.

5.2.3. If RBR operations require to grant access to Personal data that RBR Processes as the Controller to Employees or other parties (service providers), this access must be constantly monitored by the persons responsible (e.g., direct supervisors, contract owners or other persons who are responsible for the activity in question), furthermore, available amount of Personal data must be minimised as possible, including, if possible, by performing Personal data pseudonymization (concealment of personal identifiers).

5.2.4. The RBR in the form of the IT Department, Legal Department and Security Department shall control the technical resources that are used for the Processing within RBR, if necessary, by improving and replacing them with secure ones.

5.2.5. If the RBR makes Personal data available to the Employees or other authorized persons, such approach shall always be under control by making available the minimum possible amount of Personal data, including, if possible, by Pseudonymisation.

5.2.6. The RBR shall, as far as reasonably possible, ensure the ability to identify Personal data that have been Processed, the time of such processing and the person who carried it out.

5.2.7. The Employees in their workplaces and in the performance of their duties must minimise the risk of personal data being placed at the disposal of unauthorised persons, which may arise from the behaviour of the Employee: human error, theft, recklessness in the transfer of information or misuse of information resources.

5.2.8. IT and IS resources (including, but not limited to video recording software, audio, security and availability of data, password building and user monitoring, etc.) are mainly the responsibility of the IT Department which is the holder of the IT resources at RBR. Therefore, before introducing new data Processing activities, it also might be necessary to consult the IT Department on possible solutions to ensure that the Processing of the Personal Data complies with the requirements of the applicable laws. For the sake of clarity, the responsibility of the IT Department is to recommend and develop appropriate solutions if such request is raised, while it is the responsibility of the Process owner to identify a specific need and contact with the IT Department.

5.2.9. The IT Department, inter alia, will be responsible for ensuring that:

5.2.9.1. the IT and IS containing the Personal data may only be accessed by the Employees to whom the access rights have been authorized by the Process owners (to the extent information about the restrictions has been communicated by the Process Owner to the IT Department);

5.2.9.2. appropriate storage, use, operability, capacity of and protection (security) measures with respect to the IT resources and IS at the RBR (including software and hardware, related equipment, mobile phones, etc.) are implemented (to the extent information has been communicated and aligned by the Process owner to the IT Department);

5.2.9.3. technical resources are protected against disasters, i.e., fire, flooding, etc., to the extent reasonably expected of the IT Department;

5.2.9.4. prompt repair or replacement of the respective technical resources are done in time, thus ensuring that the necessary Processing operations can be carried out where needed,

5.2.9.5. restoring of operation of the IT and IS in case of any damages or other disruptions are ensured in timely manner and in accordance with the internal regulations.

5.2.10. When performing the Processing, other laws and regulations of the RBR must also be complied with, such as, procedure "Information Protection", regulation "Security Management", regulation "The Security Management of Information Technologies", "Procedure on Secure Digital Information Disposal", "IT Cryptography Requirements" etc.

5.3 CLASSIFICATION OF THE PERSONAL DATA

5.3.1. The information to be used in the activities of the RBR must be classified in accordance with the requirements incorporated in the procedure "Information Protection". The classification of information is necessary for the selection and assignment of appropriate means of information protection, ensuring the necessary confidentiality, integrity and accessibility of information assets.

5.3.2. According to Clause 27 of the procedure "Information Protection" the classification of information is provided by dividing all information in the following classes of confidentiality:

5.3.2.1. Generally accessible information;

5.3.2.2. Information for internal use only;

5.3.2.3. Limited Access Information;

5.3.2.4. Restricted Access Information.

5.3.3. In accordance with the information contained in Annex 1 "List of RBR Limited Access Information" of the procedure "Information Protection", the majority of the Personal data that are being processed at RBR are classified as Limited Access Information. Other Personal Data should be treated as Information for internal use only.

5.3.4. Safeguards for the Personal data that are classified as Limited Access Information – for Processing of such Personal data specific organizational or technical safeguards must be applied. Such Personal data can not be made available freely to all Employees of the RBR and must be available only to those Employees who need it to perform their direct work duties. The disclosure or theft of such information may cause damage to the RBR and/or the Data Subject.

5.3.5. Regardless of information contained in Annex 1 "List of RBR Limited Access Information" of the procedure "Information Protection", the Special Category Personal data and Criminal Convictions and Offences data must also be considered as Limited Access Information. Disclosure or theft of such Personal data may cause significant damage to the RBR and/or the Data Subject. Access to such Personal data must be available only to Employees who are authorised by internal regulations of the RBR or decisions of authorised representatives of the RBR, and it must be protected by enhanced security means, while the disclosure of such information requires the permission of the Management Board or of another person designated by the RBR.

5.3.6. Safeguards for the Personal data that are classified as Information for internal use only – these are Personal data regarding what no specific safeguards are applied except those that are applicable to IT and IS in general. Such Personal data are freely available to all Employees of the RBR and may be used to perform business tasks but may not be disclosed to third parties without authorisation or special permission.

5.4 THE MAIN PERSONAL DATA PROCESSING PURPOSES USED AT THE RBR

5.4.1. As mentioned in Clause 4.1.1.4 of this Procedure, Personal data must be collected for specified, explicit and legitimate purposes (Personal data Processing Purpose must be clear before a specific Processing activity is started). Comprehensive information about Processing purposes must be contained in the Processing Register. At this point, primary the Processing is being conducted for the following purposes (this list is not exhaustive since it is only intended to demonstrate the variety of purposes that can be carried used at the RBR):

5.4.1.1. The Processing of the Personal data of third parties (suppliers, service providers, Global Project stakeholders etc.), including their employees, for the purpose of carrying out the functions of RBR, including but not limited to organizing and carrying out the procurement procedures, carrying out checks on sanctions restrictions, ensuring fulfilment of the agreements entered into by the RBR, etc.;

5.4.1.2. The Processing of the Personal data of the candidates, Employees and Employees' relatives for the purposes of recruitment, staffing, development, talent management, succession planning, performance management as well as other aspects related to the employment relationship, i.e., granting benefits, extra holidays, etc.;

5.4.1.3. Video surveillance for the purposes of prevention of criminal offences related to the property, and preservation of evidence;

5.4.1.4. Implementation of marketing activities related to the core activities of RBR;

5.4.1.5. The Processing of the Personal data to carry out measures for security of critical infrastructure, or security of information or technological equipment important to the functioning of the current or future critical infrastructure.

5.4.2. The Personal data may also be Processed for a purpose other than the one of the primary purposes only if such secondary purpose is closely related to (compatible with) the primary purpose. To ascertain whether a purpose of further Processing is compatible with the purpose for what the Personal data are initially collected, after having met all the requirements for the lawfulness of the original Processing, it is necessary to take into account, inter alia:

5.4.2.1. any link between those purposes and the purposes of the intended further Processing;

5.4.2.2. the context in what the Personal data have been collected, in particular the reasonable expectations of Data subjects based on their relationship with the RBR as to their further use;

5.4.2.3. the nature of the Personal data; the consequences of the intended further Processing for Data subjects;

5.4.2.4. the existence of appropriate safeguards in both the original and intended further Processing operations.

5.4.3. For instance, it is generally always permissible to Process the Personal data for the following secondary purposes:

5.4.3.1. dispute resolution;

5.4.3.2. legal or business consulting;

5.4.3.3. for archiving purposes;

5.4.3.4. internal or independent external audits or investigations.

5.4.3.5. maintenance of the IS.

5.4.4. If the use of the Personal Data for one of the abovementioned secondary purposes has potential negative consequences for the Data subject, the RBR should take appropriate steps (such as further limiting access and taking additional security measures) to mitigate such consequences as much as reasonably possible.

5.4.5. The introduction of additional Processing purposes should be coordinated with the Legal department and the DPO, and, if necessary, records of the Processing Register must be amended accordingly.

5.5 INITIATION OF NEW PROCESSING RELATED ACTIVITIES OR CHANGES TO THE EXISTING SCOPE

5.5.1. Where it is necessary to Process the Personal data based on a purpose/method that is not listed in Processing Register or when it is necessary to change information listed in Processing Register, the Legal Department must be contacted. In such cases, the initiator of the change will have to take part in the Processing Register amendment process, e.g., it will be their responsibility to answer to all questions identified in Processing Register and other questions raised by the Legal Department. If the Process owner is not the head of the relevant department of RBR, the head of the relevant department must be consulted before any changes are initiated.

5.5.2. Heads of the departments are responsible for regular, at least annual review of information that in relation to their department is registered in Processing Register, and, if changes are found to be necessary, their implementation must be initiated in accordance with the procedures set out in Clause 5.5.1 of the Procedure.

5.5.3. If the new Processing method, especially, if it concerns new technologies and, considering Processing characteristics, context and purpose, could create a high risk to Data subject's rights and freedoms, the Process owner makes sure that before commencing new Processing related activities the DPIA is conducted. The relevant version of the DPIA questionnaire must be obtained from the Legal Department.

5.5.4. The DPIA is required at least in the following cases when operations with the following characteristics are carried out:

5.5.4.1. a systematic and extensive evaluation of the personal aspects of an individual, including profiling;

5.5.4.2. Processing of Special Category Personal data on a large scale;

5.5.4.3. A systematic monitoring of a publicly accessible area on a large scale.

5.5.5. The DPIA must include the following information:

5.5.5.1. Description of the planned Processing activity and Processing purpose, including in relevant case the Controller's legitimate interest systematic description;

5.5.5.2. evaluation on Processing activity necessity and proportionality related to purpose;

5.5.5.3. evaluation on risks to Data subject's rights and freedoms referred to in Article 35, Paragraph 1 of the GDPR; and

5.5.5.4. information on the measures for risk prevention, including guarantees, security measures and mechanisms, which ensure Personal data protection and demonstrate the compliance to the GDPR, and taking into the account Data subject and other relevant entity rights and legitimate interests;

5.5.6. After performing the DPIA, the DPIA performer prepares summary, which includes observed defects and defect prevention plan.

5.5.7. In case the Processing risk remains high after the DPIA and additional Personal data protection measure implementation (this conclusion might be reached by completing the DPIA) and, despite the risks, it is decided that the Processing in question needs to carry out, the Legal Department in cooperation with the DPO must inform Authority of such Personal data Processing and consult regarding relevant Personal data Processing performance circumstances (the RBR must provide all the information specified in Article 36 of the GDPR).

5.6 CORRECTION AND ERASURE OF THE PERSONAL DATA

5.6.1. Personal data, which are incomplete, obsolete, false, unlawfully processed are immediately corrected, clarified, or deleted and, if reasonably possible, persons, to whom the RBR had prior to that sent processed Personal data, must be informed. In case requests to rectify Personal data is received from the respective Data subject, the steps set out in clause 9.3.1 of the Procedure must be taken. If the Employee has obtained the information that the Personal data needs to be rectified in another way (by means other than those referred to in Clause 9.3.1. of the Procedure), the Employee must contact the relevant Process owner responsible for the processing of the Personal data in question and inform that a correction to the Personal data is required. After receiving the information, the Process owner must evaluate information received and, if it becomes apparent that incorrect Personal data are being processed, correct the Personal data in all relevant databases/records, if possible.

5.6.2. The Personal data, which are no longer necessary to achieve any of the purpose pursued by the RBR, must be destroyed or anonymized (i.e., altered in such a way that a Data subject can no longer be identified directly or indirectly). Electronic information shall be destroyed in such a way that it is not

possible to restore the information files. Written (paper) information shall be destroyed so that the information contained therein is not renewable. The Employee who initiates and/or carries out the Processing of the Personal Data or the person who takes over the responsibilities of such persons, must organise that the Personal Data which are no longer necessary for the fulfilment of the predefined purposes are deleted. If a request for erasure of Personal Data is received, the IT Department shall validate with the head of the department concerned that such request may be fulfilled and in case of an approval, shall perform erasure or destruction of such Personal data from data carriers (including the deletion of Personal data saved as back up).

5.6.3. Personal data that are no longer needed (not required for Personal data Processing purpose defined by the RBR) shall be irreversibly erased or destructed in such a way that it is not possible to reuse it or to identify any Personal data on it, namely paper-based Documents to be shredded before being discarded in a garbage box, Personal data containing technical resources (e.g., CD, SD, flash memory cards, hard disks, etc.) should be transferred to RBR IT department, which shall destroy technical resources in a centralized manner so that restoration of stored and deleted information would not be possible. For detailed information, see "Procedure on Secure Digital Information Disposal" and other internal laws and regulations governing the deletion of information.

5.6.4. The IT Department must ensure that the Employee shall not have the right to perform extensive erasure or destruction of the Personal data (data bases) without the order of the Management Board or unless permitted under the Procedure. An appropriate entry or deed shall be prepared with respect to any such extensive erasure or destruction.

5.6.5. An alternative to erasure of Personal data is anonymization (anonymisation is a technique applied to the Personal data to achieve irreversible de-identification, i.e., process by what personally identifiable information is irreversibly altered in such a way that a personally identifiable information principal can no longer be identified directly or indirectly, either by the RBR alone or in collaboration with any other party). Anonymization of the respective Personal data could be performed to the extent permitted under the applicable laws if there is a need for anonymised data.

5.7 INVOLVEMENT OF THE PROCESSORS

5.7.1. The RBR is entitled to entrust the Processing to person authorised by the RBR – the Processor, only in cases where the authorised Processor can perform the relevant Processing activities more effectively or in case such duty arises from another contract. It should be borne in mind that by delegating the Processing activities to the Processor, the RBR remains the main person responsible for the Processing of the Personal Data.

5.7.2. In order to begin the cooperation between the RBR and the Processor, the following conditions have to be met:

5.7.2.1. Prior to initiating cooperation and signing the partnership agreement with the Processor and during the performance of the agreement, responsible Process owner, as far as reasonably possible, checks the Processor's ability to comply with the RBR instructions for secure Personal data Processing;

5.7.2.2. Prior to delegating the Processing to the Processor, a written agreement must be signed, which includes Processor's responsibilities according to applicable laws. In exceptional cases, after obtaining the approval of the Legal department, it is allowed to use Personal data processing agreement form provided by the respective service provider if its conditions comply with the RBR and applicable law's requirements.

5.7.2.3. The Process owner, by taking into consideration the character, amount and Processing essence of transferred Personal data, evaluates necessity to perform regular inspections on

the Processor activities with the Personal data in order to ensure that it complies with the RBR's (as the Controller's) instructions for secure and partnership agreement suitable Processing.

5.7.2.4. No involvement of the Processor can be initiated without consulting the Legal Department.

5.7.3. The RBR does not allow involvement of sub-processors without written consent by the RBR. Before allowing a sub-processor to be involved, it must always be checked that the sub-processor in question will be able to ensure the security of the Processing at no lower level than that of the Processor.

5.7.4. All the new information about Processor's activities must be registered in Processing Register (info on Processors, Processor contact person, transferred Personal data types, contract periods, Personal data Processing premises and technical and organizational requirements as well as defines person responsible for partnership with the Processor in question must be shown in the Processing Register).

5.7.5. If the Personal data must be disclosed to the Processor which is located outside European Union or Europe Economic Area (in third countries), the RBR provides additional assessment and transfers Personal data to such Processors only in case one of the conditions under Chapter V "Transfers of personal data to third countries or international organisations" of the GDPR is met (for example, Personal data receiver is located in a country that provides adequate Personal data protection level; or in case there is a Data subject consent, etc.).

6. INFORMATION ABOUT THE PROCESSING OF THE EMPLOYEES' PERSONAL DATA

6.1. The RBR as the employer performs the Processing of the Employees' Personal data, observing the requirements of the applicable laws.

6.2. The purposes of the Processing of the Employees' Personal data are always closely related to the establishment, administration, fulfilment and termination of legal employment relationships. Namely, when Processing the Employees' Personal data, the following purposes are used:

6.2.1. selection of the Employees;

6.2.2. conclusion of employment contracts with the Employees;

6.2.3. provision with the necessary resources and technical equipment (for example, software, computer, phone, etc.);

6.2.4. ensuring rational use of resources of the RBR;

6.2.5. ensuring performance of statutory obligations (for example, labour protection) and rights (for example, vacation, free day for blood donors, etc.);

6.2.6. finding out the level of Employees' satisfaction;

6.2.7. ensuring corporate culture (for example, work events);

6.2.8. motivating and developing (for example, evaluation of granting additional bonuses);

6.2.9. providing information to state authorities in cases and amounts required under the applicable laws (for example, to the respective tax authority);

6.2.10. ensuring that the security requirements applicable to the RBR are met;

6.2.11. informing the funding providers about the use of the funds spent on salaries;

6.2.12. for the purposes of informing the public, the RBR may use photographs and video recordings produced by the RBR (recordings not made using day-to-day video surveillance) showing the Employee in the performance of his or her duties or in public relations activities, communications and publications, including the presentation of such events or messages on social media and social network profiles established by the RBR;

6.2.13. for the purpose of ensuring prevention of criminal offences related to the RBR's property, and preservation of evidence, video surveillance is active in the RBR's premised;

6.2.14. for the purpose of ensuring the well-being of employees

6.2.15. other purposes indicated in the Processing Register.

6.3. The RBR Processes the Personal data of the Employees only when such activity has a legal basis, for instance:

6.3.1. Employees Consent: e.g., if Employee agrees, the RBR may request feedback from the Employees former employers based on the Employee's Consent;

6.3.2. Processing is necessary for conclusion and performance of a contract to which the Employee is party: e.g., the Personal data of the Employee are necessary to sign and execute a contract (an employment contract);

6.3.3. Processing is necessary for compliance with a legal obligation to which the RBR is subject: e.g., the RBR as the employer needs to Process the Personal data of the Employee to meet the requirements of the applicable laws, e.g., requirements set out in law On State Social Insurance and law On Personal Income Tax or other applicable law;

6.3.4. Processing is necessary for the purposes of the legitimate interests pursued by the RBR: e.g., legitimate interests of the RBR include personnel resource planning, corporate culture, protection of the RBR's interests in court.

6.4. To ensure that previously mentioned Processing purposes are met, RBR needs to Process the following Personal data types of the Employee (in full or in part depending on the activities the respective Employee is involved in):

6.4.1. name, surname, personal identification number and birth date;

6.4.2. contact information (e-mail, telephone) and address;

6.4.3. information confirming identity and education, which must be presented under the provisions of the applicable laws;

6.4.4. CV and motivation letters;

6.4.5. feedback from former employers, which are being collected based on the Employee's separate Consent or other admissible legal ground;

6.4.6. results of training if the Employee attends training and educating activities provided by the RBR;

6.4.7. results of Employee's evaluations;

6.4.8. salary payments and bank accounts;

6.4.9. working hours and attendance;

6.4.10. GPS data if the Employee uses the company car;

6.4.11. a video recording if the Employee is in a video surveillance area in the RBR offices;

6.4.12. satisfaction survey results;

6.4.13. in separate cases also the Special Category Personal data might be Processed. For example, data on health are Processed to administer sick leaves, or if an accident has occurred at work. Fingerprint biometrics are Processed to ensure access to premises of the RBR;

6.4.14. Criminal Convictions and Offences data, if required by the applicable laws or otherwise in case of material and legitimate interests of the RBR, might be Processed.

6.5. The Personal data of the Employees may be transferred to:

6.5.1. an insurance company to provide the Employees with insurance related services. The RBR transfers the Personal data of the Employees to the insurance company to the extent necessary for the Employees health insurance;

6.5.2. a mobile operator to provide mobile communications services to the Employees;

6.5.3. travel agencies, airlines, hotels and apartments to organize business trips and accommodation;

6.5.4. public administration institutions in cases specified in the applicable laws;

6.5.5. distributors/owners of various software used by the RBR;

6.5.6. the RBR's cooperation partners in order to ensure that the Employees could perform their daily duties. Our cooperation partners may receive the Personal data which pertain to the Employees as the representatives of the RBR;

6.5.7. Emergency contacts indicated by the Employee;

6.5.8. entities that conduct internal or independent external audits, investigations, supervisory of the RBR's activities (for example, Ministries and their representatives).

6.6. Examples of the common Processing activities:

6.6.1. The Employees are hereby informed that based on the RBR's legitimate interests, the RBR has the right to control, record and maintain any activities performed on the part of the Employee with the RBR's property, information and communication technologies (e.g. e-mail, telephone, Internet), with a view to protecting the rights and interests of the RBR, including confidentiality, are respected, including to prevent the leakage of the Personal data and compliance with the conditions for the use of the RBR's property, information and communications technologies.

6.6.2. The Employees are hereby informed that based on the RBR's legitimate interests, company cars which are used by the Employee for the performance of their duties are equipped with a route control system (GPS) that enables route mapping for the purpose of accounting and revenues/tax reporting with a view to ensuring the protection of rights and interests of RBR.

6.6.3. The Employees' personal photograph, work anniversaries, promotions and transfers, departures, absences with a view to promoting the visibility, mutual cooperation and communication of the Employees, may be published in the internal Intranet environment of the RBR, for which only the Employees have access rights. The Employee has the right to object to such Processing and the RBR halts the Processing upon such request unless proves substantial necessity in continuing Processing.

6.7. The Employees are hereby informed that the Employees have all the same rights that are attributed to Data subjects in this Procedure, the GDPR and other applicable laws. For example, in cases where the Personal data of the Employee are Processed on the basis of the Consent of the Employee, the Employee has the right to withdraw such Consent at any time by submitting a submission via email *dpo@railbaltica.org* to RBR.

6.8. In case any of the Employees have additional questions about the Processing of their Personal data (Processing carried out by RBR), the Legal Department must be approached directly or by sending e-mail to *dpo@railbaltica.org*.

7. RIGHTS AND RESPOSIBILITIES

7.1 RIGHTS AND RESPOSIBILITIES OF THE RBR

7.1.1. In addition to the other obligations set out in the Procedure, the RBR (in the person of the Management Board, the Legal Department and/or other persons/departments of the RBR) has the following responsibilities:

7.1.1.1. The RBR must continuously evaluate and implement activities which improve the Personal data security level;

7.1.1.2. The RBR is obligated to ensure that the Processing within the RBR is performed by authorized Employees only;

7.1.1.3. The RBR shall make efforts to provide the Data subjects with easily accessible information about the Processing of their Personal data and to ensure that Data subjects are able to exercise all rights relating to the processing of the Personal Data;

7.1.1.4. The RBR records and reviews incidents, not limited to the Breaches, which have threatened the Personal data stored by or on behalf of the RBR and take them into account in the development of future policies;

7.1.1.5. The RBR must repeatedly inform the Employees about the requirements to be complied with in relation to Processing to ensure that they are fully aware of the importance and potential hazards to the security of the Personal data and that they are qualified enough to comply with the Personal data protection related laws.

7.1.2. In addition to the other rights set out in the Procedure, the RBR (in the person of the Management Board, the Legal Department and/or other persons/departments of the RBR) has the following rights:

7.1.2.1. The RBR may unilaterally restrict authorised Employee access to the IT and/or Information systems containing Personal data without notice if the authorised Employee violates this Procedure or any applicable laws;

7.1.2.2. The RBR is entitled to request a written confirmation of compliance and confidentiality requirement observation while working with Personal data and the Information systems;

7.1.2.3. The RBR reserves right to request information related to fulfilment of their duties from Employees involved in the Processing, to the extent such information is related to the Processing;

7.1.2.4. If this cannot be agreed by amicable means, the Legal Department RBR on behalf of the RBR shall determine who is the respective Process owners and register such Process owner in the Processing Register;

7.1.2.5. The Legal Department on behalf of the RBR is entitled to impose additional obligation of confidentially while working with the Personal data, which shall be binding to an Employee during the employment or other type of relationship with the RBR. The Employees might be asked to ensure that such obligations also apply to the authorized personnel of the Processor;

7.1.2.6. The Legal Department on behalf of the RBR is entitled to draft and approve changes in the Processing Register, DPIAs and other registers that might be needed in relation to the Processing;

7.1.2.7. The RBR is authorized to change the provisions of this Procedure, subject to approval by the Management Board and notification to the Employees.

7.2 RIGHTS AND RESPOSIBILITIES OF THE EMPLOYEES AND PROCESS OWNERS

7.2.1. The Employees inter alia have the following responsibilities with respect to the Processing:

7.2.1.1. To request and obtain timely access to the IT and IS necessary for the performance of their duties related to the Processing;

7.2.1.2. To handle the Personal data that they can access with strict confidentiality and not to Process such data without authorisation. The Employee may only Process the Personal data within the scope necessary to fulfil their duties. When in doubt, the Employee may turn to the Legal Department;

7.2.1.3. If the Employee requests access to Personal Data, the Employee must proactively provide a proper justification explaining why such access is necessary;

7.2.1.4. To provide assistance in investigating the Breaches;

7.2.1.5. To be familiarized with the requirements of the Procedure and other procedures that are closely linked to the fulfilment of obligation arising from this Procedure;

7.2.1.6. To reduce the risks of unauthorised access to Personal data, which may be caused by human error, theft, inadvertency during information transfer or incorrect use of the IT. For example, the Employee must always make sure that the information containing the Personal data on the Employee's computer screen is not visible to others;

7.2.1.7. To perform other responsibilities prescribed under the Procedure, other internal governance documents or the applicable laws as well as reasonably related to such responsibilities;

7.2.1.8. To ensure that all the Documents (including in paper form) that contain Personal data are stored in such a way that they are not available to third parties, including other Employees who do not need to work with the relevant Documents. Similarly, if the workplace is located in such a way that there is a large flow of people around it, the Documents on the work surface shall be placed in such a way that their content is not visible and as unattainable as possible to third parties.

7.2.1.9. Employee who identifies that Processing is not in line with the Procedure must immediately report such non-compliance by sending an email to dpo@railbaltica.org.

7.2.2. The Employee is strictly prohibited to:

7.2.2.1. Carry out activities that endangers the security of the information containing the Personal data;

7.2.2.2. compile Personal data in large databases, unless the creation of such databases arises out of the performance of work duties;

7.2.2.3. Transfer technical resources to third parties if they contain the Personal data unless proper safeguard and the Processing principles are taken into account (this prohibition should also be observed in cases where IT resources are handed for disposal).

7.2.3. The Employee inter alia has the following rights with respect to the Processing:

7.2.3.1. To request availability of the IT and the IS resources needed for the fulfilment of the requirements of this Procedure;

7.2.3.2. To obtain explanations regarding the access restrictions to the IT and/or the IS resources;

7.2.3.3. To make proposals to improve the security of the Personal data;

7.2.3.4. To request advice and training in relation to the applicable laws and security of the Processing of the Personal data.

7.2.4. In addition to the aforementioned, the Process owner has the following responsibilities in relation to the Processing processes in their supervision:

7.2.4.1. to define/review the means and purposes of the Processing (relevance, necessity etc.);

7.2.4.2. to develop/review the regulating procedure/instruction/policies of process if the nature of Processing requires a special procedure / instruction / policies;

7.2.4.3. to make sure that RBR has implemented a mechanism allowing to obtain information, where necessary, about which Data subjects' Personal data have been Processed and how it is done. If such a mechanism is not developed/available, Process owner must initiate its development and must implement it together with other colleagues from other departments of RBR;

7.2.4.4. to engage in an assessment process, if one is to be carried out, to assess Data subjects' requests;

7.2.4.5. to assess received complaints related to the Processing in cooperation with the Legal Department and the DPO;

7.2.4.6. to assess and provide suitable partner (Processor) selection, contract closing and supervision, in case there is a need for involvement of the Processors;

7.2.4.7. to participate in Personal data security incident (not limited to Breaches) examination, risk identification, damage control and future measure development in order to prevent further risks as well as oversee the necessary works;

7.2.4.8. to be updated in circumstance and regulation changes, which might affect the Processing for intended purpose and, in the case of such changes, check the relevance and adequacy of Processed Personal data type.

7.2.4.9. to provide training to Employees under its control in relation to Processing activities that are under the responsibility of the Process owner, where this would be considered as a necessary and an appropriate measure;

7.2.4.10. to initiate and participate in DPIA process;

7.2.4.11. to define Employee's categories which can have access to the Personal data in the Process owner`s supervision;

7.2.4.12. to develop suitable technical and organizational measures for the Processing, including Personal data delegated to Processors, in cooperation with other departments of the RBR (IT, Legal Department etc.).

8. PERSONAL DATA BREACHES

8.1 ACTIONS OF THE EMPLOYEES IN RELATION TO THE BREACHES

8.1.1. All Employees are required to familiarise themselves with the Procedure to be able to: (a) identify all types of potential Breaches; (b) carry out their respective competencies indicated in the Procedure; and (c) as far as possible, to make all necessary steps to prevent the Breaches.

8.1.2. If, however, the Breach has occurred and discovered, the Employee shall report immediately, but not later than within 3 (three) hours from the moment of discovery, to the Legal Department and Security Department by sending an e-mail to dpo@railbaltica.org, indicating in the e-mail the information on

the Breach, the existing or potential consequences of the Breach, as well as information on the actions (if any) taken or proposed to prevent, terminate, or mitigate the consequences of the Breach. As far as reasonably possible, the Employee is responsible to ensure that implementation of the actions necessary for the prevention or cessation of the alleged Breach and for the mitigation or elimination of its effects are conducted.

8.1.3. The Employees is obliged to report regarding any Breach, irrespective of the cause of the Breach, including if:

8.1.3.1. the Breach occurred as a result of the conduct of the Employee him/herself;

8.1.3.2. the Employee noted the alleged infringement of the conduct of another Employee;

8.1.3.3. information is received from the Data subject or the Processors (partners);

8.1.3.4. publicly available information is received;

8.1.3.5. the Breach is discovered by auditors.

8.1.4. Within the limits of his or her competence, the Employees must actively cooperate with persons who are involved in the Breach investigation and must take all reasonable steps to cease the Breach which has already occurred, and to eliminate or mitigate its adverse effects, while at the same time ensuring that information on circumstances relevant to the Breach (evidence) is not destroyed.

8.1.5. The Employees should note that committing of the Breach may lead to civil, administrative or criminal liability.

8.2 OBLIGATIONS OF THE LEGAL DEPARTMENT

8.2.1. Upon receiving information on the Breach, the Legal Department must:

8.2.1.1. get involved in the Breach investigation;

8.2.1.2. take actions that ensure suspension, prevention and mitigation of the Breaches;

8.2.1.3. report about the respective Breach to the Corporate risk manager, and, where relevant, to the IT Department or other department of the RBR;

8.2.1.4. make an entry in the Breach Register;

8.2.1.5. ensure that DPO is immediately informed about the respective Breach;

8.2.1.6. ensure, where necessary, notification of the Breaches to the Authority;

8.2.1.7. perform other duties specified in the Procedure, other binding documents and the applicable laws.

8.2.2. The Legal Department shall register the Breach in the Breach Register as soon as reasonably practicable after the receipt of respective information. The Breach Register must be drawn up by Legal Department no later than the moment when the first Breach is reported, and it must be drafted by Legald Department.

8.2.3. Without undue delay, the Legal Department shall organise the required activities so that the Breach is rectified or terminated, and the adverse effects of the Breach are eliminated or mitigated if such actions have not already been performed by the Employee who reported the Breach.

8.2.4. The Legal Department shall assess whether the Breach may pose a risk to the rights and freedoms of the Data subject. During the assessment, the DPO's opinion on the assessed risks, adverse effects of the Breach and advises on further actions, as far as reasonably practicable, shall be taken into account.

8.2.5. Considering the DPO's opinion, the Legal Department shall take a decision on the notification of the Breach to the Data subject and/or the Authority and shall proceed with notification if such is the decision. The decision to notify the Data subject and/or the Authority must be communicated to the Management Board before the notification process is initiated.

8.2.6. The Legal Department, when taking the final decision as indicated in Clause 8.2.5 of the Procedure, in particular takes into account the following circumstances:

8.2.6.1. the risk posed by the Breach to the rights and freedoms of Data subject(s);

8.2.6.2. the technical and organisational protection measures implemented and the appropriateness of these measures for the Personal data affected by the Breach, particularly those which make the Personal data incomprehensible to persons who do not have the power to access data, such as encryption;

8.2.6.3. the measures taken and their ability to ensure that the high risk of the rights and freedoms of the Data subject(s) does not materialise;

8.2.6.4. the technical possibilities for notification to the Data subject;

8.2.6.5. the outcome of the consultations with the DPO.

8.2.7. In case it is decided that the Authority must be informed, a notification to the Authority must be performed by submitting a notification using online tool or the special template of the notification published by the Authority, all of which are available on the website of the Authority (https://pazinojums.dvi.gov.lv/).

8.2.8. The notification to the Data subject must be made in a clear and simple language, by means of a statement or, where this would require disproportionate efforts, by means of public communication or a similar measure, and, among other things, must include the following information:

8.2.8.1. The potential adverse effects of the Breach;

8.2.8.2. The measures taken by the RBR to prevent and mitigate the consequences of the Breach;

8.2.8.3. Measures which are desirable to be taken by the Data subject in order to mitigate the potential adverse effects of the Breach;

8.2.8.4. The name and contact details of the DPO or other contact person who could provide additional information.

8.3 COMMON TYPES AND EXAMPLES OF THE BREACHES

8.3.1. All Breaches might be classified in three types:

8.3.1.1. *Privacy violation* (the most common type of the Breaches): the Employee collects the Personal data illegally (collection is not allowed), discloses it unlawfully (data is accessed, disclosed or transferred to an unauthorized person) or Processes the Personal data in another illegal way, for instance:

I. When a person finds out the access password of another person because it is not sufficiently protected and accesses the respective Information system and looks at the data (makes a copy).

II. Sending an e-mail containing the Personal data to the wrong recipient.

III. Disclosing the Personal data to a person without identity verification (e.g., by telephone).

IV. Transferring the Personal data to other Employees, but such Personal data are not necessary for the performance of the respective duties by such other Employees.

V. Loss (including theft) or leaving a Document containing the Personal data without supervision in a readily accessible place to third parties.

VI. Internal Information systems are accessed by third parties as a result of IT security vulnerabilities or suspicious (phishing, etc.) e-mails.

VII. Loss of a portable working computer or other portable device – even if the Personal data on the device is a backup copy.

8.3.1.2. *Integrity breach*: the Personal data are altered or destroyed by accident or by an unauthorized person, for instance, when a person learns the access password of the other person because it is not sufficiently protected and accesses the respective Information system and changes the data.

8.3.1.3. *Accessibility breach*: a physical or technical disruption resulting in the loss of access to the Personal data by the responsible persons, for instance:

I. Lost access to electronically stored Personal data as a result of electricity breakdown, cyber-attack or other technical factors.

II. Lost access to the Personal data stored in paper Documents as a result of loss of the Document safe key, fire or other physical factors.

9. DATA SUBJECT'S REQUESTS AND COMPLAINTS

9.1 GENERAL REQUIREMENTS APPLICABLE TO THE PROCESSING OF DATA SUBJECTS' REQUESTS

9.1.1. According to the Chapter III of the GDPR (Rights of the data subject), Data subjects have several rights that the RBR must respect. For example, the Data Subjects might request to: (a) provide information on Processing of their Personal data; (b) edit their Personal data; (c) delete his/her Personal data; (d) limit Processing of their Personal data; (e) ensure their Personal data portability.

9.1.2. The Data subject may submit a request to the RBR in person, by mail or electronically via e-mail. In general, the RBR accepts written requests from identifiable Data subjects.

9.1.3. The Data subject's requests may always be fulfilled only if the Data subject who request performance of the action is identifiable.

9.1.4. If the requests are given orally, they may be accepted in person from Data Subjects or notarially authorised representatives of Data Subjects while making a written note of the essence of the request. After the orally expressed request has been recorded in writing, it must be given to the Data Subject or his authorised person for signature.

9.1.5. If the request is submitted in classical written format and in person, then it has to be signed with wet ink and the submitter must be the Data subject. If the request is submitted electronically, it has to be signed with secure electronic signature.

9.1.6. In case if the request is submitted by third party on behalf of the Data subject, request must contain authorisation (i.e., notarially approved power of attorney) which provides third person with right to perform the action in question.

9.1.7. In case a written request is received, the Legal Department checks the identity of person, regarding which the Data subject's request is sent. If it is not possible to identify Data subject, the Data subject's request submitter is asked to provide additional information for the identification of Data subject.

9.1.8. The RBR gives response to the Data subject's request in one of the following means:

9.1.8.1. by posting it to the address provided by the Data subject in the respective request;

9.1.8.2. by providing the Data subject with information in person;

9.1.8.3. in other way that is convenient to the Data subject, by reviewing each case individually. If this approach is used, the following aspects must be assessed: the amount of information to be provided, the possibilities of personal identification and the security of the data transfer channel in order to prevent an unauthorised disclosure of Personal data to third parties.

9.1.9. On receipt of the first written inquiry (submission) from the Data subject, the Legal Department prepares the Data subjects request register (if possible, it must be incorporated in electronic document management system used by RBR), which ensure Data subject's request records, response preparation deadline monitoring as well as allow the RBR to identify excessive requests which enables to request administrative fee for Data subject's request fulfilment.

9.1.10. Irrespective of the type of request received from the Data subject, the Legal Department registers such request the Data subjects request register and ensures that a response is prepared within one (1) month. If it is not possible to provide response within one (1) month for objective reasons, the RBR can extend the response deadline to three (3) months (in total), by informing Data subject on extension within one (1) month after submission of the request.

9.1.11. The rights of the Data subjects identified in Paragraph 9 "DATA SUBJECT'S REQUESTS AND COMPLAINTS" of the Procedure may be restricted only in specific cases specified in the applicable laws.

9.1.12. All communication with Data subject and information provision to Data subject must be performed free of charge except for cases when requests are obviously unjustified or excessive. In such cases, the RBR may refuse to fulfil the request or request reasonable administrative fees related to information provision.

9.1.13. All heads of RBR's departments are required to prepare responses to Legal Department queries relating to Data Subject Requests within 5 (five) working days or within a different timeframe if that is explicitly approved by the Legal Department.

9.2 DATA SUBJECTS' REQUESTS TO PROVIDE INFORMATION ON THE PROCESSING

9.2.1. In case the Data subject requests to provide information on Processing of their Personal data, the Legal Department follows the following pattern:

9.2.1.1. collects information on Personal data in the RBR disposal, including verifying the RBR database information, information stored on servers, information in paper format (for example, cooperation agreements) and other storage places.

9.2.1.2. ensures that when preparing data copy requested by the Data subject, collected information do not contain third party's (other Data subject's) Personal data. In such case these data are to be deleted and not provided to the Data subject in terms of execution of relevant rights.

9.2.1.3. if the RBR does not possess relevant Data subject's Personal data, such a reply must be given to the data subject. It is unacceptable that the response to the Data Subject is not provided at all.

9.3 DATA SUBJECTS' REQUESTS TO RECTIFY THEIR PERSONAL DATA

9.3.1. In case Data subjects request to rectify their Personal data, the Legal Department follows the following pattern:

9.3.1.1. verifies whether Personal data mentioned in the request differ from the Personal data processed by the RBR.

9.3.1.2. prior to fulfilling the Data subject's request, the Employee responsible for responding to the request verifies whether Personal data should be clarified, in other words, whether the information in question are indeed wrong or is it only Data subject`s opinion.

9.3.1.3. If the RBR can not agree on rectification of the Personal data, the Employee responds to the Data subject by mentioning reasons why data will not be rectified.

9.3.1.4. If it is assessed that Personal data are to be rectified, the Employee in charge performs modifications as soon as possible.

9.3.1.5. If the RBR may rectify Data subject's Personal data, the Employee verifies whether rectified Personal data are transferred to third party and, if it is not excessively complicated, informs relevant Personal data receivers on rectification.

9.3.1.6. If the RBR does not possess relevant Data subject's Personal data, the Employee responsible for responding to the request prepares a suitable response, mentioning, that the RBR has not processed Data subject's Personal data.

9.4 DATA SUBJECTS' REQUESTS TO DELETE THEIR PERSONAL DATA

9.4.1. In case Data subjects request to delete their Personal data, the Legal Department follows the following pattern:

9.4.1.1. deletes such Personal data only in the following cases:

I. the RBR no longer requires Personal data mentioned in the request for the purpose they were collected and processed except the cases, when prolonged Processing is required by the applicable laws, archive needs or for the protection of the RBR's legitimate interests (for example, legal proceeding risks);

II. if the Processing of Data subject's Personal data is performed based on Data subject consent and it is revoked;

III. if Processing of Data subject's Personal data is performed based on the RBR legitimate interests and Data subject justifiably objects to such data Processing by pointing out significant reasons to stop such Processing;

IV. if the Processing of Data subject's Personal data is performed for direct commercial marketing purposes, including profiling as far as it is related to direct commercial marketing;

V. if the Processing of Data subject's Personal data was unlawful;

VI. if the Personal data are to be deleted according to regulatory requirements applicable to the RBR.

9.4.1.2. informs the Data subject on request fulfilment.

9.4.1.3. If the RBR deletes Data subject's Personal data, verifies whether deleted Personal data are not transferred to third party and, if it is not excessively complicated, informs relevant Personal data receivers on deletion.

9.4.1.4. If the RBR does not possess relevant Data subject's Personal data, the Employee responsible for responding to the request prepares a suitable response, mentioning, that the RBR has not processed Data subject's Personal data.

9.5 DATA SUBJECTS' REQUESTS TO LIMIT PROCESSING OF THEIR PERSONAL DATA

9.5.1. In case Data subjects request to limit Processing of their Personal data, the Legal Department follows the following pattern:

9.5.1.1. limits the Processing only:

I. for the duration of time while the RBR verifies justification of requests in case of dispute of Personal data accuracy;

II. for a duration specified by the Data subject if he/she has objected to deletion of Data subject's Personal data in case unlawful Processing has been observed;

III. for duration specified by the Data subject, if the RBR no longer requires to store Personal data, while, respectively, the Data subject requires them to make, implement or defend legal claims;

IV. for a duration of time while the Data subject's justifications to stop the Processing, which is based on RBR's legitimate interests, is verified.

9.5.1.2. If the Processing is limited, ensures that the relevant Personal data are used only for storage, the RBR or third-party legal claim implementation and defence, the member state's essential interests or in separate cases when Data subject has consented Processing of the Personal data under limitation.

9.5.1.3. If the RBR has limited Processing of Data subject's Personal data, it verifies whether Personal data under limitation have not been transferred to Third party and, if it is not excessively complicated, informs relevant Personal data receivers on limitation.

9.5.1.4. If the limitation is to be cancelled, the RBR informs the Data subject before the limitation is cancelled.

9.5.1.5. If the RBR does not possess relevant Data subject's Personal data, the Employee responsible for responding to the request prepares a suitable response, mentioning, that the RBR has not processed Data subject's Personal data.

9.6 DATA SUBJECTS' REQUESTS TO PROVIDE PERSONAL DATA PORTABILITY

9.6.1. In case Data subjects request to provide their Personal data portability, the Legal Department follows the following pattern:

9.6.2. If the RBR processes relevant Personal data, the Employee responsible for fulfilment of the request verifies whether the relevant Personal data portability is executable, in other words, verifies whether relevant Personal data:

I. are processed based on the Data subject's consent or contractual obligation fulfilment;

II. are processed in electronic medium.

9.6.3. If the RBR possesses Personal data, which can be portable (incl. their transfer to another destination required by the Data subject), the Employee responsible for responding to the request prepares relevant Personal data in electronic format (*.xml, *.doc, *.csv) and provides them to the Data subject or Third party authorised by the Data subject.

9.6.4. If the Data subject has specified that Personal data are to be transferred directly to Third party, the RBR reviews amount of Personal data to be transferred and decides on suitable security measures for requested information transfer by encrypting the information using password or other solutions for secure information transfer. It should be ensured the other person's privacy is not compromised by ensuring Data subject's rights, , including, no other Data subject data shall be transferred without justification.

9.6.5. If the RBR does not possess relevant Data subject's Personal data, the Employee responsible for responding to the request prepares a suitable response, mentioning, that the RBR has not processed Data subject's Personal data.

9.7 THE RBR'S RESPONSE IN CASE A COMPLAINT IS RECEIVED FROM THE DATA SUBJECT

9.7.1. When a complaint from the Data subject regarding the Processing of their Personal data is received, the Legal Department performs the following activities:

9.7.1.1. If the RBR does not Process the Personal data of the relevant Data subject, Employee responsible for responding to request prepares a suitable response, mentioning, that the RBR has not processed that Data subject's Personal data.

9.7.1.2. If the RBR processes relevant Personal data, the Employee responsible for responding to the complaint review the complaint together with the DPO and prepares the answer.

9.7.1.3. if the RBR is found to have conducted the Breach, the rules applicable to the Breaches that are mentioned in this Procedure must be complied with.

10. ROLES AND RESPOSIBILITIES

Performer / Task (this list is not exhaustive)	Legal Department	Employees	Process owners	IT Department	Security Department
On a day-to-day basis reviews the actions taken by themselves to ensure that Processing activities are carried out in accordance with this Procedure	C	R	C		C
Within the scope of his/her competence, supervise the compliance of other Employees with the requirements applicable to Personal Data Processing	R		R		R
Provides all the necessary information at the request of the Legal Department (where it is necessary to comply with obligations under the Procedure/GDPR)		R	A	C	C
Provides support for the correct application of this Procedure by organizing trainings and direct consultations	R				
Ensures that the Procedure contains up-to-date information and amends it where necessary	R				
Directly communicates with the DPO	R				
Maintains the Processing Register and advises on the entries it contains/needs (cooperates with the Process owners)	R				
Responsible for ensuring that the Legal Department has all the necessary information to make proper entries in the			R		

Processing Register and initiates preparation of the DPIAs, where needed					
Ensures that responses to Data Subjects are prepared	R				
Responsible for IT and IS resources that are used for the Personal data Processing within the RBR	C			R	C

R – Responsible, A - Accountable, C-Consulted, I – Informed.

11. CLOSING PROVISIONS

11.1. Upon the entry into force of this Procedure, the following procedures shall cease to have effect:

11.1.1. "Procedure for the Determination, Prevention and Notification of Personal Data Protection Violations" (approved by Management Board's decision No 19/20/2019 on 01 April 2019);

11.1.2. "Internal rules for the protection of the processing of personal data" (approved by Management Board's decision No 18/20/2019 on 01 April 2019).

REFERENCES

Ref:	Document Number:	Document Title:
1.	**Internal Governance Documents**	
1.1.	RBGL-SCR-PRC-Z-00001	Information Protection Procedure
1.2.	1.11/10.7	Regulation on Security Management
1.3.	RBGL-SCR-RGL-Z-00002	Regulation on the Security Management of Information Technologies
1.4.	RBGL-RBR-STN-Z-00007	Secure Digital Information Disposal Standard
1.5.	RBGL-RBR-STN-Z-00006	IT Cryptography Requirements Standard
1.6.	RBCR-RBR-XX-XX-REG-Z-00001	Processing Register
2.	**External Referenced Documents**	
2.1.	2016/679	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)
2.2.	OP number: 2018/132.1	Personal Data Processing Law