RISEBA
Biznesa, mākslas un tehnoloģiju
AUGSTSKOLA

APPROVED
19 March 2021. Rector's Order
No. 21/1.1-3/30

General Personal Data Protection Policy

I. GENERAL PRINCIPLES OF PERSONAL DATA PROTECTION

I.I. DEFINITIONS AND ABBREVIATIONS

Company/RISEBA	SIA "Biznesa, mākslas un tehnoloģiju augstskola "RISEBA"" (reg. No. 40003090010), its structural units, branches, representative offices, affiliated companies and associations.
Management	RISEBA Rector; Vice-Rector for Academic Affairs; Vice-Rector for Research; Vice-Rector for Development; Director of Finance and Administration
Immediate supervisor	The company representative specified in the relevant employee's employment contract or appointed by an Order as the employee's direct manager.
Employee	Any person with whom the Company has an employment relationship, including the immediate supervisor
DPO	RISEBA data protection specialist, dpo@riseba.lv
Third party	A natural person, legal person, public authority, agency or body other than the data subject, the controller, the processor and persons authorised by the controller or processor to process personal data.
Data subject	Natural person
CSC	RISEBA Customer Service Centre
Regulation	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.
RISEBA website	riseba.lv; victoria.riseba.lv; architecture.riseba.lv.
Cooperation partners	Suppliers, clients, invited specialists, service providers, etc.
External specialist	A natural or legal person who provides services or supplies products on the basis of a concluded contract.
Special categories of data	Data relating to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data for the purpose of uniquely identifying a natural person; health data; and data concerning a natural person's sex life or sexual orientation.

I.II. DATA PROCESSING PRINCIPLES

RISEBA is committed to processing personal data in accordance with the Regulation, as well as other legislation governing privacy and data processing matters.

Personal data obtained in the course of RISEBA's activities is processed in accordance with the following principles:

a. Data is processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");
b. Data is collected for specific, explicit and legitimate purposes, and is not further processed in a manner incompatible with those purposes ("purpose limitation");
c. The data must be adequate, relevant and limited to what is necessary for the purposes for which they are processed ("data minimisation");
d. The data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");
e. Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation");
f. processed in a manner that ensures appropriate security of personal data ("integrity and confidentiality");
g. processed in a manner that ensures the controller's ability to demonstrate compliance with all principles ("accountability").

I.III. GENERAL PROVISIONS

a. This policy applies to all personal data processed by RISEBA, its departments, affiliated associations and companies.
b. The policy is binding on every RISEBA employee.
c. Personal data is stored or transferred in paper, physical and electronic formats, or communicated verbally in conversation or by telephone.
d. This policy applies to any employee who obtains, stores, or has access to personal data and uses it.
e. This policy applies to all locations from which personal data is accessed, including in the context of remote working.
f. Policy also applies to RISEBA's international activities, which take the form of cooperation and agreements with foreign partners in other jurisdictions, as well as attendance at international events.
g. The Policy is applied in conjunction with any other policies, provisions, orders, procedures and/or guidelines adopted and implemented by RISEBA.
h. This policy is reviewed at least once a year.

I.IV. LAWFULNESS, FAIRNESS AND TRANSPARENCY

a. To ensure that personal data is processed lawfully, fairly and in a manner that is transparent to the data subject, RISEBA records the processing activities carried out under its control.
b. The record of processing activities is reviewed at least once a year.
c. RISEBA ensures that data subjects' personal data is used for legitimate purposes and in accordance with data subjects' reasonable expectations;
d. RISEBA implements data subjects' rights to access their personal data and promptly considers data subjects' requests.

I.V. LEGAL BASIS FOR DATA PROCESSING

a. RISEBA processes personal data on the following legal bases:

- The data subject's consent;
- Data processing arises from the data subject's contractual obligations or, at the data subject's request, is necessary for the conclusion of a relevant contract;
- Processing is necessary to comply with a legal obligation to which RISEBA is subject;
- Processing is necessary to protect the vital interests of the data subject or another natural person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in RISEBA;
- Processing is necessary for the purposes of the legitimate interests pursued by RISEBA or 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 personal data, in particular where the data subject is a child.

b. The relevant legal basis for each type of data processing is specified in the record of processing activities.
c. Where the processing of personal data is based on the data subject's consent and such consent is held by an employee, the employee shall ensure that proof of such consent is stored together with the relevant personal data or transferred to the DPO.
d. If the proof of consent is stored together with the personal data, the employee shall, upon request by the DPO, provide information on its location.

I.VI. DATA MINIMISATION

RISEBA ensures that the personal data being processed is:

a. adequate – sufficient and limited to what is necessary to achieve the purposes of processing;
b. relevant – the data has a rational connection to the purpose of processing;
c. contains only the necessary data and is not stored for longer than necessary.

I.VII. ACCURACY

a. RISEBA undertakes to take reasonable measures to ensure the accuracy of personal data. Each employee is responsible for ensuring that the personal data processed is accurate.
b. Depending on the nature of the legal basis for processing, the employee shall take steps to ensure that the data subject's personal data is kept up to date.

I.VIII. RIGHT OF ACCESS

Access rights to documents containing data subjects' personal data are granted only in accordance with the employee's duties, as set out in the employment contract concluded with the employee and the job description attached thereto. Access by employees and persons not justified by the requirements of regulatory enactments, the job description or a specific Order is not permitted.

I.IX. DELETION OF PERSONAL DATA

a. RISEBA undertakes to delete personal data:

- if the data is no longer being processed;
- if the data is being processed unlawfully;
- if the data subject withdraws their consent, except where further processing is justified by the interests of RISEBA or another person, which override the rights and freedoms of the data subject.

b. To ensure that personal data is not stored for longer than necessary, RISEBA, when processing personal data, sets retention and erasure periods for each type of processing.
c. It must not be possible to restore data that has been deleted in a timely manner.
d. A situation where personal data is deleted before the specified period must not be permitted. In case of doubt, the deletion of personal data must be agreed with the line manager and the DPO.
e. Paper documents containing personal data shall be destroyed by shredding.

I.X. TECHNICAL AND ORGANISATIONAL DATA SECURITY MEASURES

RISEBA undertakes to comply with and maintain the following data security measures:

a. Security on the RISEBA premises is ensured by a security company and/or CCTV cameras and/or restricted access to office premises, which is ensured by the CSC key issuance Procedure, under which a key is issued to each employee personally.
b. At the end of the working day, offices are locked and keys are handed over to the CSC.
c. Third parties are not permitted to be present in RISEBA offices without the presence of the relevant office employee.
d. For the processing and storage of personal data, RISEBA endeavours to utilise the latest technological advancements and organises the physical storage of data in such a way that the data is not destroyed, lost, altered, or subject to unauthorised disclosure or access;
e. When data is stored in any physical form, RISEBA ensures secure storage, taking into account available resources and the requirements of regulatory acts relating to the storage of the specific type of data.
f. To minimise the risk of data disclosure, staff carry out data anonymisation and pseudonymisation where possible.
g. Access to personal data is granted to employees on a need-to-know basis. When granting such access, specific instructions from the immediate supervisor, other employees or a Specialist regarding data protection and dissemination are always followed to prevent the unauthorised downloading, copying, sharing or deletion of personal data.
h. Appropriate backup and security breach response solutions are implemented. Each instance of a breach is duly documented.
i. The ability to effectively restore lost personal data is ensured through the use of secure and reliable information technology solutions.
j. If personal data is transferred to countries outside the European Union or the European Economic Area, RISEBA ensures that such transfers take place only in accordance with the provisions set out in the Regulation.
k. When using external data storage devices (USB sticks, discs or other devices) to transfer personal data, the employee ensures that the data is securely deleted from the storage device as soon as the transfer is complete

I.XI. SECURITY BREACHES

a. RISEBA undertakes to manage data security breaches by taking all necessary measures to minimise the impact of consequences related to personal data.
b. Every security breach and the measures taken to address it are recorded in the relevant breach log.
c. In the event of a physical or technical security breach resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, RISEBA undertakes to immediately assess and mitigate the risks to the rights and freedoms of data subjects.
d. In cases where the provision set out in the Regulation applies, RISEBA undertakes to report the personal data breach to the Data Protection Authority, as well as to the data subjects.
e. In the event of a security breach, or where there are doubts regarding the security of personal data or its unlawful disclosure, an employee is obliged to report this immediately to the DPO (dpo@riseba.lv) and their Line Manager.

II. EMPLOYEE DUTIES AND RESPONSIBILITIES

II.I. ALL RISEBA EMPLOYEES WHO PROCESS PERSONAL DATA HAVE THE FOLLOWING OBLIGATIONS:

a. to ensure that the Data Protection Specialist is properly and promptly involved in all matters relating to the protection of personal data;
b. where translation of data protection documentation is required, to submit a translation request to the DPO and not to translate it themselves or engage any other translation specialist;
c. participate in relevant RISEBA training sessions, information events and assessments, which are developed and implemented to promote compliance with this Policy and RISEBA's overall compliance with data security provisions;
d. familiarise themselves with RISEBA's security guidelines and policies and comply with their requirements in their day-to-day work;
e. take all necessary measures to ensure that their actions do not result in data security breaches;
f. adhere to the 'clean desk' principle, which stipulates that when working with personal data during the working day, only those documents necessary for the performance of the current task should be left on the desk. At the end of the working day, no documents or data storage devices containing personal data may be left on the desk.
g. Inform RISEBA in a timely manner of any changes to your personal data that was provided to RISEBA within the framework of an employment or cooperation relationship.
h. Report any security breach immediately, or in cases where there are doubts regarding the security of personal data or its unlawful disclosure;
i. In the event of any doubts regarding the security of personal data or its unlawful disclosure, or in the event of a security breach, the employee is obliged to report this immediately to the DPO and their line manager.

II.II. DUTIES OF LINE MANAGERS

All line managers are responsible for the timely implementation of this Policy within their organisational unit **("Department")** and for ensuring compliance with the Policy's provisions by their subordinates, which includes:

a. Familiarising themselves with the Department's data processing provision and ensuring compliance;
b. Defining responsibilities and tasks for data protection management within the Department;
c. Managing access rights to personal data to ensure that employees have access only to the personal data necessary for the performance of their duties;
d. Ensuring that all Department staff participate in the relevant training and assessments provided by RISEBA and DPO, and that each staff member is aware of their responsibilities in the field of personal data protection;
e. Assist DPO in maintaining an accurate and up-to-date register of data processing activities.

II.III. EMPLOYEE RESPONSIBILITIES

An employee is liable for any failure to comply with this Policy and/or DPO guidelines and instructions. An employee shall bear all losses incurred by RISEBA as a result of failure to comply with this Policy and/or DPO guidelines and instructions, which causes RISEBA material losses, administrative or criminal liability, damage to reputation, or any other outcome that negatively affects RISEBA's business operations.

The Employee shall only be held liable if RISEBA can prove that the Employee has breached, failed to comply with or disregarded the provisions of this Policy and/or DPO guidelines and instructions.

III. PROCESSING OF EMPLOYEES' PERSONAL DATA

III.I. WORKING TIME RECORDING

In view of RISEBA's legal obligation to accurately record the total hours worked by each employee, as well as separately overtime, night work, work during weekly rest periods and work on public holidays, line managers keep records of their department's employees' working hours, which are reconciled with the Human Resources Department each month and submitted to the Accounting Department.

Working time records, as well as their electronic copies, are stored and processed in accordance with the retention periods specified in the Records Classification Scheme and the requirements of regulatory acts.

III.II. INTERNAL COMMUNICATION AMONG STAFF

For the purposes of work organisation and to the extent necessary to ensure that employees are reachable, can communicate effectively with one another and perform their duties, RISEBA uses the following methods of internal communication: employee contact details, email communication, surveys and polls, as well as the RISEBA intranet.

Employee contact details

Employee contact details are made available by regularly sending an updated list of telephone numbers to all employees via their work email. The list of telephone numbers contains the following data: the

employee's first name, surname, position, office number, internal telephone number, landline number, and the corporate mobile telephone number assigned by RISEBA. An employee's personal mobile phone number is included only if the employee's consent has been obtained.
Contact details are published and used for as long as the legal employment relationship with the employee exists. Taking into account the number of staff, staff turnover and rotation, the list of telephone numbers is updated at least once every two (2) months.
The department responsible for updating the data is the Human Resources Department. Employees and the responsible department, each within the scope of their respective responsibilities, ensure that contact details are up to date and updated as necessary.

Communication via email

When communicating electronically, the following data security conditions must be observed:

1. The transmission of unnecessary personal data must be avoided;
2. Do not send data to persons not specifically associated with the personal data in question;
3. Avoid creating unnecessary copies;
4. Where possible, replace email correspondence and the storage of data therein with other technological solutions, such as shared sites or the intranet.

Surveys and polls

When conducting employee surveys and inviting staff to take part in votes, employees must be informed of:

1. how the data collected will be used, and
2. whether participation is voluntary, and
3. whether the employee's participation is anonymous or identifiable.

III.III. CORPORATE NUMBER AND EMAIL POLICY

Upon entering into an employment relationship with RISEBA, the Employee is assigned a RISEBA corporate email address and a landline telephone number. For the performance of their duties, each Employee may apply to receive a RISEBA corporate mobile phone number. The allocation of a number is agreed and approved by the Line Manager.

The number assigned to the Employee (as well as the RISEBA email address) shall not be considered the Employee's private personal data, as it is used to contact the Employee in their professional capacity. As the Employee's telephone number and email address are considered to be data of the RISEBA legal entity, the provisions of the Regulation regarding the processing of such data do not apply.

III.IV. CORPORATE CULTURE

The implementation of RISEBA's corporate culture is considered to be in RISEBA's legitimate interests, and the processing of employees' personal data within this framework is considered to be processing for the purposes of legitimate interests. RISEBA's corporate culture is implemented through measures that include, but are not limited to: the presentation of recognition and awards, the use of employees' personal data on social media, and the organisation of corporate events.

Awards and recognition

As part of its corporate culture, RISEBA awards employees with prizes and recognition with the aim of promoting interaction among employees, as well as facilitating the achievement of the goals set by both employees and RISEBA.
For the purpose of awarding awards and other recognition, RISEBA processes the following personal data of employees: employees' performance and achievements at work, education attained, and awards and recognition received elsewhere; achievements outside the workplace that relate to the employee's competence and job duties; and feedback from colleagues.
Given the public nature of the awarding of awards and recognition, photographs and video recordings capturing the employee's award ceremony may only be published and made available to third parties if the employee has given their prior consent. In accordance with RISEBA's data processing provision, an employee's consent to the use of their photographs and video recordings is obtained when the employee enters into an employment relationship with RISEBA and/or prior to a specific event, upon registering for it.
Every employee has the right to decline to be nominated for an award.
When collecting or providing feedback on an employee who is nominated for an award or recognition, it is prohibited to collect or disclose the employee's sensitive data, and ethical standards must be observed.

Corporate events

To promote adherence to values, RISEBA regularly organises and holds corporate events with the aim of fostering and strengthening staff cohesion, motivation and mutual communication. Such events include, but are not limited to: RISEBA anniversaries, Latvian national holidays and international commemorative days, sports games, and other special RISEBA events.

Given that photographs and video recordings are taken at many events, personal data of employees visible in photographs and video recordings may only be published and made available to third parties if the employee has given their prior consent. In accordance with RISEBA's data processing provision, an employee's consent to the use of their photographs and video recordings is obtained when the employee enters into an employment relationship with RISEBA and/or prior to a specific event, upon registering for it.

With the aim of making the recordings available to staff, and in certain cases to promote RISEBA's image, RISEBA publishes the photos and videos on its website and/or social media, and information regarding the location of the recordings is sent to staff via email.

In cases where family members of employees are also invited to attend RISEBA events, information regarding the public nature of the event is included in the event announcement, and consent for the use of photographs and video recordings is obtained prior to the specific event – either during the registration process or by displaying information at the event venue.

Given that identifying employees' family members for the purpose of complying with the Regulation's provisions regarding the provision of information to data subjects requires disproportionate effort and may unjustifiably restrict the observance of RISEBA's legitimate interests, the registration of family members for the event and informing them of the public nature of the event and the data processing provisions is considered to be the responsibility of the employee.

If the nature of the event requires the provision of Special Category Data to RISEBA, the processing of an Employee's family member's data requires the consent of the family member themselves. An employee organising such an event shall, prior to sending invitations to employees, inform RISEBA DPO of the need to process special category data of employees' family members.

The interests of employees' minor children regarding the processing of personal data shall be represented by the employee.

Provided that all the information measures specified here have been implemented, the attendance of the employee and their family members at the event will always be deemed to constitute their consent to the event's provisions.

Social media

For the promotion of RISEBA's image and as part of marketing campaigns, employees' personal data may be used on RISEBA's social media platforms, in advertising campaigns, and in other ways dictated by elements of corporate culture.

An employee has the right, on grounds relating to their particular situation, to object at any time to the processing of their personal data by sending a request to dpo@riseba.lv. RISEBA will cease processing personal data, except where there are compelling legitimate grounds for processing that override the employee's interests, rights and freedoms, or where the processing is necessary for the establishment, exercise or defence of RISEBA's legal claims.

IV. PROCESSING OF STUDENTS' PERSONAL DATA

IV.I. STUDY PROGRAMMES

When developing study programmes, for each study programme, only those types of documents and information are assessed and specified that are necessary for the student to apply for it and for RISEBA to ascertain the student's suitability for the programme and compliance with its provisions. The list of documents to be submitted for a study programme does not include excessive data that is not of decisive importance in assessing the student. Therefore, the amount of data to be submitted varies for each study programme, corresponding to the programme's objectives and specific nature.

IV.II. ACCESS RIGHTS AND DATA RETENTION PERIODS

Access to students' academic records is restricted to those staff members who require such information to perform their duties and in accordance with the provisions specified in the relevant section.

Attendance records

When recording attendance, staff do not collect excessive personal data, but record only the data necessary to ensure the accurate and error-free recording and identification of students.

To record attendance, the lecturer uses a specially designed attendance record form.

Retention period for attendance records: attendance record sheets are retained until the student's assessment is prepared and for 1 year after the final assessment has been carried out, with the aim of ensuring sufficient evidence in the event of student complaints.

Legal basis for the processing of personal data: performance of a contract, legitimate interests.

Exams and reports

Student internship reports and course papers are retained by the Faculty department (with the Programme director) for 1 year and, upon expiry of the retention period, transferred to the RISEBA archive. Justification for the retention period: in the event of a student's complaint – to ensure RISEBA is informed regarding the grounds and circumstances of the complaint. Upon expiry of the retention period, personal data is permanently deleted and destroyed.

Exam records are compiled and retained for the duration of all students' studies, as well as for 1 year after graduation. During a student's studies, exam records are retained by the lecturer and the Study Programme Administrators.

Reason for the retention period: to provide evidence and supporting information in the event of a student's complaint.

Provision on the retention of educational documents

Documents certifying education are retained in accordance with Paragraph 19 of Provision No. 451 "Procedure for the Issuance of State-Recognised Documents Certifying Vocational Education and Professional Qualifications and Documents Certifying the Completion of Parts of Accredited Vocational Education Programmes":

"Forms for vocational education educational documents, unissued vocational education documents, the register of the issue of vocational education documents, the register of vocational education document forms and all documents relating to the receipt of forms shall be stored in a fireproof, locked safe."

Other accounting documentation

Registers of the issue of vocational education educational documents, examination records, summary records of academic performance and other accounting documentation, as well as their electronic copies, shall be stored and processed in accordance with the time limits specified in the File Nomenclature and the requirements of regulatory enactments.

Once the provisions for retention periods have expired, the records are destroyed or transferred to the archive.

V. PROCESSING OF PARTNERS' DATA

RISEBA ensures the secure processing of the personal data of Cooperation Partners and their employees.

RISEBA processes the following personal data of CPs, as well as personal data that CPs provide to RISEBA or that RISEBA receives from public authorities and sources:

V.I. PERSONAL DATA OF COOPERATION PARTNERS – NATURAL PERSONS:

Type of data	**Purpose of processing**	**Legal Legal basis**	**Data retention period**	**Data recipients/ Access rights**
Data subject's first name, surname, personal identification number, position, address, bank account details	a) Contractual relationship (including performance of contractual obligations, invoice processing, communication, legal and compliance activities); b) Marketing communications.	6(1)b; 6(1)c (contractual relationship) Article 6(1)f (marketing communications)	For the duration of the contract; In accordance with the requirements	• Accounting Department; Marketing Department; Customer Service Centre; • External service providers; • State Revenue Service.

* Article 6(1)(b) of the Regulation – processing is necessary for the performance of a contract to which the data subject is a party, or for taking steps at the request of the data subject before entering into a contract.
Article 6(1)(c) of the Regulation – processing is necessary for compliance with a legal obligation to which the controller is subject.
Article 6(1)(f) of the Regulation – processing is necessary for the legitimate interests pursued by the controller or by a third party.

V.II. PERSONAL DATA OF EMPLOYEES OF COOPERATION PARTNERS

RISEBA processes the following personal data of employees of cooperation partners: first name, surname, position, and work contact details.

Taking into account Recital 14 of the Regulation and the fact that the personal data of employees of CPs is not considered to be the employees' private personal data, as well as the fact that RISEBA processes such data solely for business purposes, the requirements of the Regulation regarding the processing of such employees' personal data do not apply.

The Regulation also does not apply in situations where a CP employee uses personal contact details in the course of their duties. Given that RISEBA's obligation to verify the ownership of each email address is considered an excessive burden and administrative burden on RISEBA, Cooperation partners are themselves responsible for the contact details they provide within the framework of the cooperation, as

well as for the procedures governing the use of their employees' personal means of communication and contact details.

V.III. PARTICIPATION IN RISEBA EVENTS

In the context of events organised by RISEBA, as well as for the purposes of staff training, RISEBA may invite specialists with various areas of expertise to participate in or lead events.

The employee organising such an event shall ensure that all data security requirements are met and shall therefore inform RISEBA DPO of the need to process personal data before sending an invitation or signing a contract with the Specialist.

This obligation applies in particular where it is planned to take photographs or make video recordings at such an event and to use the resulting recordings subsequently as part of RISEBA's marketing strategy.

VI. PROCEDURE FOR PROVIDING INFORMATION AND TRANSFERRING DATA

VI.I. REQUESTS FROM THIRD PARTIES

Staff shall ensure that the personal data and information regarding RISEBA students, trainees and other staff (hereinafter – Data Subjects) are not disclosed to other persons in person or via email, except where such disclosure is required by law. The disclosure of Data Subjects' personal data by telephone is prohibited.

When disclosing documents and information containing the personal data of Data Subjects, the Employee shall verify the identity of the recipient.

The disclosure of documents and information to other persons not related to the specific data subject, such as parents (unless the data subject is under 18 years of age), journalists, etc., is not permitted.

When personal data of Data Subjects is requested by foreign authorities and organisations, the Employee must ensure that the following Procedure for information, documents and references containing personal data is followed before the disclosure of data:

- **If the request comes from a Latvian authority or organisation:** The Employee processing such requests and preparing responses must only disclose the requested information if the submitted request is justified by the requirements of Latvian legislation. In all other cases, the Employee must obtain the specific Data Subject's consent.

- **If the request comes from a public authority or organisation in an EU and/or EEA country**:
  - by email – the Employee processing such requests and preparing responses must only provide the requested information if the submitted request is signed with an electronic signature, or if another procedure stipulated by legislation has been followed. Otherwise, it is prohibited to disclose the Data Subject's personal data.
  - by post – The employee processing such requests and preparing responses must, taking into account the likelihood, circumstances and available resources, and using reasonable efforts, ensure that such a request is:
    - drawn up in accordance with the prescribed procedure – the request is submitted

by a genuinely existing institution and is based on a specific regulatory act, the requirements of which can be verified;
- signed – it is signed by an authorised signatory of the institution; and
- stamped – if this requirement applies in the country of origin of the request.

Otherwise, it is prohibited to disclose the data subject's personal data.

❖ **If the request comes from a country outside the EU and the EEA**:

- by email – it is not permitted to provide the Data Subject's personal data. To examine the request and prepare a response, the Employee must contact the DPO.
  by post – the provisions applicable to requests submitted by post by organisations located in the EU and the EEA must be followed (see the previous point).

Upon receiving a request that does not meet the aforementioned criteria, the Employee is obliged to immediately inform the DPO thereof, providing full details of the request and a description of the circumstances, and must cooperate with the DPO in preparing a response.

In any event, the Employee shall not be limited to the aforementioned procedure but shall utilise other options available to them, even if not mentioned in this procedure, to ensure that the request received is lawful and that there is no risk to the rights and freedoms of data subjects.

In case of any doubt, the Employee must contact RISEBA DPO (dpo@riseba.lv).

VI.II. TRANSFER OF PERSONAL DATA TO THIRD PARTIES

In accordance with the requirements of regulatory acts, as well as the principles and provisions set out in the Regulation, Employees may transfer Data Subjects' personal data to the following recipients:

- state and local government authorities,
- service providers.

When transferring the personal data of Data Subjects to partner companies and service providers, the Employee must ensure that a contract for the processing of personal data and/or a confidentiality agreement has been concluded with such parties. If no agreement has been concluded, the Employee must contact the DPO, providing full details of the nature and duration of the cooperation, the cooperation partner or institution, and must cooperate with the DPO in drafting the agreement.

If cooperation with third parties involves the transfer of documents containing the Data Subject's personal data, the Employee shall, as far as possible, ensure that the documents are transferred without the Data Subject's personal data. For example, when submitting a contract for translation, the Data Subject's personal data must be removed from the contract: first name, surname, personal identification number, residential address, etc.

If cooperation with third parties involves third parties accessing documents containing the Data Subject's personal data, the Employee shall, to the extent possible, endeavour to minimise the disclosure of personal data where such disclosure is not related to the purpose of the cooperation.

VII. ORGANISING EVENTS

When organising an event, the Employee is obliged to contact DPO to ensure the lawful processing of the personal data of event attendees. This obligation applies to events of any type, size and significance – annual celebrations, public lectures by guest speakers, excursions, etc.

An employee organising an event is obliged to ensure the involvement of the DPO before addressing the event participants. When sending a request to the DPO, the following must be specified:

- A description of the event;
- Categories of event attendees (staff, students, partners, etc.);
- The purpose of using personal data obtained during the event or in the course of organising the event;
- The language of the event.

If translation of the data protection documentation is required, the Employee shall submit a translation request to the DPO and shall not translate it themselves or engage any other translation specialist.

VII.I. PARTICIPANT REGISTRATION

If participant registration is scheduled to take place during the event, the Employee responsible for the event shall ensure that the participant registration forms are submitted to the DPO immediately after the event, but no later than one week after the date of the event.

Paper and electronic forms of participant registration shall be retained in accordance with the purposes for which the information contained therein is used, as follows:

1) Purpose of personal data processing: registration of participation, sending reminders about the event; Types of personal data: first name and/or surname, email address; Legal basis for the processing of personal data: legitimate interests; Retention period for personal data: 2 months.
2) Purpose of personal data processing: sending RISEBA news and announcements; Types of personal data: first name and/or surname, email address;
   Legal basis for processing personal data: consent;
   Duration of personal data processing: indefinitely, until the individual withdraws their consent or unsubscribes from receiving news.

VII.II. PHOTOGRAPHY AND VIDEO RECORDING

Where prior registration of participants is required for attendance at an event and the event participants are limited to those who have received an invitation or invitation from RISEBA, and where photography and/or video recording is planned during the event, the staff member responsible for organising the event shall ensure that a warning regarding the taking of photos and video recordings is included in the registration form.

Where prior registration is required for participation in the event and the participants also include third parties

who received an invitation or call to attend from RISEBA indirectly, and where photography and/or video recording is planned during the event, the staff member responsible for organising the event shall ensure that the registration form includes a warning regarding the taking of photographs and video recordings, and shall ensure that a sign warning of the taking of photographs and video recordings during the event is displayed at the entrance to the event.

Where no prior registration of participants is required for attendance at the event, but photography and/or video recording is planned during the event, the Employee responsible for organising the event shall ensure that a sign warning of photography and video recording during the event is displayed at the entrance to the event.

In the event that a sign warning of photography and video recording is displayed at the entrance to the event, the Employee responsible for organising the event shall photograph the sign displayed at the event, which shows the event or the entrance to it and which can be identified later, and shall send this photograph to DPO atdpo@riseba.lv immediately after the event, but no later than one week after the date of the event.

The warning sign shall be prepared and provided by DPO.

VIII. CCTV

Video surveillance is carried out at RISEBA with the aim of ensuring the protection of the life, health and property of RISEBA staff and visitors, as well as preventing and detecting criminal offences. The purpose, method and means of video surveillance, the persons responsible for the processing and protection of personal data obtained as a result of video surveillance, the retention period for video recordings and other provisions are set out in RISEBA's internal provisions.

Video surveillance is not used to monitor Employees. RISEBA ensures that no excessive or inappropriate personal data is collected during video surveillance, and that the viewing angle of the installed cameras does not cover Employees' workstations.

Due to RISEBA's legal obligations, video surveillance recordings may be handed over to state law enforcement authorities in accordance with the procedures laid down in legislation.

The internal provisions on video surveillance and the assessment of the necessity of video surveillance are reviewed once a year.

IX. RETENTION PERIODS FOR PERSONAL DATA

RISEBA stores and processes data subjects' personal data in accordance with the time limits and procedures set out in the provisions, as well as RISEBA's file classification system.

When the processing of personal data is no longer necessary to fulfil provisions set out in a contract or by law, or the data processing period has expired, the Employee shall remove the personal data from all systems and records, irrevocably deletes and destroys the data and/or takes measures to anonymise it appropriately so that the data subject can no longer be identified, unless RISEBA is required to retain personal data to fulfil legal or regulatory obligations, or to preserve evidence in the event of an investigation into a breach.

If no retention period for personal data is specified in a regulatory act or the Case Nomenclature, personal data must be retained for as long as is necessary to achieve the purpose of the processing of personal data. With regard to the processing of personal data for which the data subject has given consent, personal data shall be processed until such consent is withdrawn or until the date specified in the consent form.

If there are any doubts regarding the retention period and legal basis, staff are obliged to contact the RISEBA data protection Specialist (dpo@riseba.lv).

X. DATA SUBJECT REQUESTS AND COMPLAINT HANDLING PROCEDURE

X.I. DATA SUBJECT REQUESTS

In accordance with the provisions of the Regulation, RISEBA is obliged, without undue delay and in any event within one month of receiving the data subject's request, to inform the data subject of the action taken in response to their request, taking into account the data subject's rights as set out in the Regulation.

If RISEBA does not take the action requested by the data subject, RISEBA shall, without undue delay and at the latest within one month of receiving the request, inform the data subject of the reasons for not taking such action and of the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

The processing of data subjects' requests and complaints, as well as the preparation of responses, is carried out by RISEBA DPO. Upon receiving a data subject's request or complaint regarding their personal data, the Employee shall immediately inform the DPO of such a request, attaching a description of the situation as well as other information related to the specific personal data.

X.II. EMPLOYEE REQUESTS

Employees may send questions or complaints regarding the processing of personal data to RISEBA DPO at:dpo@riseba.lv. In order for an Employee's question or complaint to be investigated, the Employee must provide full details of the nature of the situation, specifying in the email the circumstances of the personal data processing breach.

In the event of an Employee's complaint, RISEBA is obliged, without undue delay and in any event within one month of receiving the Employee's request, to inform the Employee of the action taken in response to their request, taking into account the data subject's rights as provided for in the Regulation. If necessary, this period may be extended by a further two months, taking into account the complexity and number of requests.

If the Employee's requests are manifestly unfounded or excessive, in particular because of their repetitive nature, RISEBA may either:

a) charge a reasonable fee, taking into account the administrative costs associated with providing the information or communication or carrying out the requested action; or

b) refuse to comply with the request.

XI. DUTIES OF THE DPO:

a. compile information on the compliance of the data protection process and submit a report on the reporting period to the Rector of RISEBA once a year;
b. organise training on the protection of employees' personal data at least once a year;
c. inform and advise RISEBA and employees who carry out processing of their obligations under the Regulation and other provisions on data protection;
d. monitors compliance with the Regulation, other data protection provisions and RISEBA's Policy on personal data protection, including the allocation of responsibilities, the provision of information and training to staff involved in processing activities, and related audits;
e. provides advice on data protection assessments and monitors their implementation;
f. cooperates with the supervisory authority;
g. act as the CPP for the supervisory authority on matters relating to data processing;
h. provides advice on any other matters.