

Guidelines for the Notification of Personal Data Processing to Data State Inspectorate¹

First of all you have to evaluate if it is necessary for you to notify personal data processing to Data State Inspectorate:

Question 1 – Do you process personal data?

Yes, continue with the question 2.

No, there is no need for you to notify the personal data processing.

Personal data – any information related to an identified or identifiable natural person. For detailed information please see the recommendation of Data State Inspectorate - “Personal Data Definition”.

Processing - any operation carried out regarding personal data, including data collection, registration, recording, storing, arrangement, transformation, utilisation, transfer, transmission and dissemination, blockage or erasure.

Question 2 – Are you the controller?

Yes, continue with the question 3.

No, then you don't need to register.

Controller - a natural person or a legal person, state or local government institution that determines the purposes and the means of the personal data processing, as well as is responsible for the personal data processing in accordance with Personal Data Protection Law.

Question 3 – Are you registered in the Republic of Latvia or is the personal data processing carried out outside the territory of the Republic of Latvia that belongs to the Republic of Latvia in accordance with international agreements or technical equipment is located in the Republic of Latvia that is being used for personal data processing, except in those cases when the equipment is being used just for the transfer of personal data through the territory of the Republic of Latvia?

Yes, continue with the question 4.

No, then you don't need to register.

Question 4 – Do you process the personal data just for the personal, family or household purposes; furthermore you do not and will not make these personal data known to a third party?

Yes, then you don't need to notify.

No, continue with the question 5.

¹ Please note that personal data processing notification form should be filled out in Latvian and submitted to Data State Inspectorate.

Question 5 – Do you process personal data for such purposes:

- ⊙ it is foreseen to transfer the personal data that is not the European Union member state or the member state of the European Economic Zone;
- ⊙ it is foreseen to process the personal data in order to provide financial services, to carry out market or public opinion research, to select or evaluate personnel as entrepreneurship if it is provided as a service to other companies/ state institutions/ natural persons, raffling or lotteries;
- ⊙ the information on persons' health is being processed;
- ⊙ personal data processing is related to crime, criminal record and cases of administrative infringements.

Yes, it is necessary to notify the personal data processing to Data State Inspectorate (see the information available on the website of Data State Inspectorate on how to notify personal data processing);

No, continue with the question 6.

Question 6 – Do you:

- ⊙ process personal data for bookkeeping and personnel record keeping purposes;
- ⊙ process personal data within the information systems of state and local government institutions and the data gathered there are publically available;
- ⊙ process personal data for the journalistic purposes in compliance with the Law on Press and Other Mass Media;
- ⊙ process personal data for archiving purposes in compliance with the Law on Archiving;
- ⊙ process personal data within a religious organization;
- ⊙ carry out the personal data processing in accordance with the chapter 1 (data subject consent) and chapter 2 (data processing derives from contractual agreements of the data subject or considering the request from the data subject the processing for personal data is necessary to conclude the corresponding agreement) of the Article 7 of the Personal Data Protection Law or Article 13.¹ (identification code of the person) of this Law;
- ⊙ carry out personal data processing for the needs of scientific, statistic, genealogical research?

Yes, you don't need to notify the Data State Inspectorate.

No, continue to the question 7.

Question 7 – Have you registered the data protection officer in Data State Inspectorate?

Yes, you don't need to notify the personal data processing to Data State Inspectorate.

No, it is necessary for you to notify personal data processing to Data State Inspectorate (see the information on the website of Data State Inspectorate – how to notify the personal data processing).

How to register personal data processing in Data State Inspectorate?

1. Fill out the application form (available on the website of Data State Inspectorate) where the purpose or purposes for data processing have to be indicated. In case it is necessary, you should draw up a power of attorney that approves the fact that the person who signs the application form is authorised to represent the legal person or an institution submitting the application form.

2. Pay the state tax for the notification of the personal data processing. The state tax should be paid before you hand in the notification application.

The state tax is 40 lats for the notification of personal data processing. If the controller is a natural person or the micro enterprise corresponding to the definition determined by the Commission **Regulation (EC) No.364/2004** of 25 February 2004 amending **Regulation (EC) 70/2001** as regards the extension of its scope to include aid for research and development (Attachment No.1), the state tax is 20 lats.

The bank account for the payment of the state taxes:

Recipient: State Treasury
 Registration No.: 90000050138
 Account No. **LV51TREL1060190913600**
 Receiving institution: State Treasury
 The BIC of the receiver: TREL LV22

3. Send the notification application form (if necessary also the power of attorney) by mail, e-mail that has been signed with the secure electronic signature or bring it personally to the office of Data State Inspectorate (Blaumana street 11/13-15, Riga). The documents in the office of Data State Inspectorate are accepted every working day from 8:00-12:00.

Data State Inspectorate provides paid services for the filling out and printing out the form of personal data processing – 25 lats.

Data State Inspectorate considers the notification application for personal data processing within 30 days. If it is necessary to clarify the information indicated at the application form, Data State Inspectorate sends a letter to the applicant. Once receiving the necessary additional information, Data State Inspectorate takes a decision to notify or to refuse the notification of personal data processing. At the same time when the decision for the notification of personal data processing is provided, the notification certificate is handed out to the controller or his/ her

authorised person **in person** at the office of Data State Inspectorate.

Once Data State Inspectorate has taken the decision, the contact person indicated in the personal data processing notification application form is being informed about it immediately.

Filling out of the application form of personal data processing

Date – indicate the date when the document is being signed (day, month, year).

Place – indicate the place where the document has been elaborated, issued, adopted or signed. The place where the document has been elaborated, issued, adopted or signed has to correspond to the official title of the place according to the administrative territory.

1. The controller – indicate the natural or legal person, the institution that determine the aim of the personal data processing and the means of processing, as well as is **responsible** for the personal data processing in accordance with the Personal Data Protection Law (for instance, a company “Saulite”, its unified registration number, full title).

2. Contact information – indicate the legal address, phone number, e-mail address, fax number of the controller.

3. Personal data processor – indicate the authorized person (another authorized organization, legal or natural person based on contractual agreement) of the controller that on behalf of the controller carries out the assignments and with whom a contract in writing has been concluded regarding the personal data processing. The processor is not an employee of the controller’s company.

Here also indicate the goal/ goals that are determined in the above mentioned contract and the operator has to achieve within the concluded contract.

If the personal data processing is carried out just by the controller, then in this field indicate “*Don’t have*” and the contact information at the point 4 should be crossed out.

4. Contact information – in case you have the personal data processor, indicate his/ her contact details here (legal address, phone number, e-mail address, fax number).

5. Contact person on the notification issues of personal data processing – indicate the name, surname and contact information of the responsible person whom to contact regarding the issues of personal data processing notification.

6. Information on personal data processing

Please, note that in case personal data are processed for several purposes, fill out the point 6 of this application form regarding every personal data processing purpose separately. Then attach the information regarding the point 6 of the application as an attachment/ attachments to personal data processing form.

6.1. The purpose of personal data processing – indicate precise, comprehensive purpose of personal data processing (for example, record keeping of clients in the hotel for service provision purposes, record keeping of job seekers for the purpose of arranging job abroad).

6.2. Legal grounds for personal data processing – indicate what the legal ground for personal data processing is.

The legal ground for personal data processing can be the **Article 7 point** of Personal Data Protection Act or **the Article 11 point** of the Personal Data Protection Act (processing of sensitive personal data).

In case the legal ground is **the Article 7 point 3** of the Personal Data Protection Act, then indicate the legal act that foresees the corresponding personal data processing.

6.3. Categories of data subjects – indicate comprehensive categories of natural persons that can be directly or indirectly identified (for example, clients, patients, employees, etc.)

6.4. Types of personal data – indicate all types of personal data that you will be processing (for example, name, surname, personal code, diagnosis and education, etc.)

6.5. The categories of personal data recipients – indicate those natural or legal persons that will receive the data indicated in point 6.4. of this application form (for example, the data subject about himself/ herself, the potential employer of the data subject, credit management companies, authorized employees of the controller, etc.)

6.6. The foreseen type of personal data processing – mark with

electronically manually mixed (both types mentioned).

Indicate 'mixed' in case personal data is processed both on paper and electronically.

6.7. Way of obtaining personal data – indicate how the personal data are going to be obtained (for example, during interviews, from questionnaires, contracts, etc.)

6.8. Place of personal data processing – indicate the personal data storage address/addresses (for example, place where the server is located).

6.9. Holder of information resources – indicate the employee of the controller who is responsible for the usage of information resources (system programmes, application software, data files and other information processed in personal data processing).

6.10. Holder of technical resources - indicate the employee of the controller who is responsible for the usage of technical resources (computers, computer network and other technical equipment used for the personal data processing).

6.11. Responsible person for information system security - indicate the employee of the controller who ensures and is responsible for access to information and who ensures integrity and confidentiality.

6.12. Transfer of personal data to other countries - mark with

Personal data will not be transferred to the countries which are not the member states of the European Union and the European Economic Zone.

Mark with the in case when you do not transfer the personal data to the above mentioned countries, as well as in cases when the personal data at all will not be transferred to another country.

Personal data will be transferred to the following countries that are not the countries of the European Union and the European Economic Zone.

Indicate the full official name of the countries.

For example: 1. Russian Federation;
2. The United States of America;
3.

Types of personal data to be transferred to the countries that are not the member states of the European Union and the European Economic Zone.

Here indicate what type of personal data will be transferred to the countries mentioned above.

For example:

1. name, surname, personal code;
2. name, surname, personal code, residence address;
3.

7. Have the adequate technical and organisational activities that ensure personal data protection been introduced?

Yes/ No

The mandatory technical and organisational requirements for personal data protection are determined by the Cabinet of Ministers regulations No 40 of 30 January 2001 “The Mandatory Technical and Organizational Personal Data Protection Requirements”.

In case the adequate technical and organisational activities have been introduced, then answer on the following questions:

7.1. Have the internal protection rules been elaborated?

Yes/ No

Within these rules you have to determine:

- the person (persons) responsible for personal data protection;
- personal data protection classification according to the value and confidentiality level of the data;
- technical resources – how the personal data processing would be ensured;
- organisational order of personal data processing (time, place, procedural issues);
- activities that should be carried out in order to ensure the protection of the technical resources in cases of emergencies (fire, flood).
- means how to ensure the technical resources against direct damage and its illegal obtainment;
- order regarding the storage and destruction of the information carriers;
- conditions for the length and construction of the password;
- order regarding the usage of passwords, time frame when the password has to be changed.
- action to be taken once the password or the crypto-key has been made known to a third person.

7.2. Has the internal annual personal data processing audit been carried out:

The audit of personal data processing – regular and independent investigation. During this investigation it is being determined whether the activities related to the

personal data processing are in compliance with the requirements of the legal acts in the field of personal data protection and with the internal personal data protection security requirements elaborated by the controller.

Internal personal data protection audit – the organisation itself carries out the personal data processing audit.

The controller carries out the internal personal data processing audit annually and elaborates a report regarding the activities carried out in the sphere of information security.

State and local government institution once in two years submit to Data State Inspectorate the audit report on personal data processing, including the risk analysis and the report on the activities carried out in the field of information security.

7.3. During the last three years has there been an external personal data processing audit carried out?

Yes/ No

External personal data processing audit – Data State Inspectorate or an independent consultant (auditor) carries out the personal data processing audit within an organisation.

7.4. Have all the necessary means and activities been implemented in order to secure you against unauthorised or illegal personal data processing, as well as against accidental data loss or damage?

Yes/ No

7.5. Is the control of physical protection ensured?

Yes/ No

Control of physical protection – the protection of technical resources against the threat constituted to information system by physical impact (for example, fire, flood, theft of technical resources, air temperature, and improper temperature of the air determined by the operational instruction).

7.6. Is the access control to personal data introduced?

Yes/ No

Indicate if there is a person who is supervises the possibilities of other persons to get access to personal data (for example, distribution of rights, passwords, and crypto-keys).

7.7. Has the continuity plan of the system operation been introduced or the continuity plan of the institution (enterprise) operation?

Yes/ No

7.8. Is the training provided to the employees on the security of systems and procedures and personal data protection?

Yes/ No

7.9. Are the security incidents investigated and discovered?

Yes/ NO

7.10. Are the information system security standards introduced?

Yes/ NO

In case the answer is “Yes”, indicate the numbers and the titles of the standards introduced.

8. Is the information mentioned in this application form related to all your personal data processing that is necessary to be notified to Data State Inspectorate in accordance with the Personal Data Protection Law?

Yes/ NO

Please note!!! This is an approval that all the information that you have indicated in this application form relates to all the personal data processing that you are carrying out.

9. Authorised person of the controller – fill it out if the application form is signed by the authorised person of the controller.

Please indicate, what is the legal ground for this person to sign the application form (for example, a power of attorney). Once submitting the application form, the document that confirms the signatory powers also has to be attached (if necessary).

10. Approval

By signing this approval you acknowledge that all the information provided by this application form is true. You should be aware of the fact that by providing the information that is not true, you will be made answerable according to the legal acts.

11. Signature

Indicate the name, surname, signature of the person, who signs the application form, as well as the place where the document was elaborated, issued, adopted or signed and the date when the document was signed (date, month, and year).

Please note!!! **Cross out** all the columns that you did not fill out. Please **number** and **sew together** all the pages of the application form.