

Data protection conditions

APPROVED

by Order No 108
of Director of 19 August 2019
Annex

Data protection conditions of the Centre of Registers and Information Systems

Information on the processing of personal data has been compiled in accordance with Article 12 of the [General Data Protection Regulation 2016/679 of the EU](#) [1] titled “Transparent information, communication and modalities for the exercise of the rights of the data subject” in order to comply with the requirements of a controller and principles of processing personal data, as well as for notifying natural persons of the enforcement of rights.

1. These data protection conditions do not cover the following:

- the storage of legal entities’ data and processing of personal data on third party websites referred to on the RIK website (external links);
- the purposes, scope and methods of public registers and information systems managed by RIK, and of processing of personal data, the conditions for making such data publicly available, and the rights and procedure for access to personal data provided by law ([Land Register Act, Commercial Code](#) [2], etc.) or regulations adopted under the statutory mandate (Order No 24 of the Minister of Justice of 30 June 2010 “Internal rules of the land registry department”, etc.)

2. RIK processes your personal data when you:

- visit the RIK website;
- visit the social media pages of RIK on Facebook and LinkedIn;
- apply to work for us (or have worked for us);
- submit an information request, request for clarification or memorandum to us;
- contact our helpdesk (NB: the phone calls are recorded);
- visit the Centre of Registers and Information Systems.
- Your data has been entered into the accounting software e-Financials (we act as the controller of the database).

2.1.1 Visiting the RIK website

When you visit the RIK website, the personal data collected and stored about you is limited to the following:

- IP address of the computer or computer network used;
- web browser and operating system of the computer;
- time of visit (time of day, date, year).

RIK does not link the collected IP addresses to any particular visitor. Statistical data is collected on which part of the website you visit and how much time do you spend there. Such data is used to prepare visitor statistics, so that it can be used for improving the website and to make it more user-friendly. The data will be stored for three months.

2.2.1 Use of social media channels Facebook (including the English version) and LinkedIn

We have activated the following settings for the purposes of using our Facebook page and LinkedIn:

- the page is visible to everyone;
- we have limited the option of posting on our wall;
- the comments can be added in all languages; we have also enabled automatic translation of posts to readers who speak other languages;
- people can contact us privately via Facebook;

2.3.1 Applying for a job or internship at RIK

Information on job and internship vacancies can be found on the [RIK website](#) [3].

When you apply for a job or an internship at RIK, we use the personal data you have submitted only for the following purposes:

- to evaluate your job application;
- to evaluate your qualifications and to make decisions concerning the hiring process;
- to communicate with you, for example, to notify of the potential dates of the job interview;
- to prepare basic reference materials, which are used in case you are hired.

The candidate's personal data is processed by the employees participating in the recruiting process. Other employees of RIK have no access to the personal data of candidates.

Personal data of candidates is collected upon submission of documents required in the job/internship listing, while:

- the data used originates from the information disclosed by the candidate themselves and from public sources (including social networks, blogs, public register data, such as from the Criminal Records Database, the Commercial Register, court decisions, etc.);
- the candidate has the right to know what kind of data RIK has collected about him or her;
- the candidate has the right to access the data collected by RIK, as well as provide explanations and submit objections;
- we assume that the candidate has provided their consent for the persons included in their references listed in the application documents to answer questions concerning the applicant, and that the references have consented to RIK contacting them for information.
- Your data will not be disclosed to other candidates and the data of other candidates will not be disclosed to you.

The data of candidates is considered to be data with a restriction on access to which third parties (including competent authorities) can access only in cases established in legislation.

We store correspondence concerning employment relationships, personnel, etc. for five years. We store internship contracts, authorisation agreements and employment contracts for ten years of the termination of the contract. After that period, the relevant documents are destroyed.

2.4.1 Submitting an information request, request for clarification or memorandum

RIK uses your personal data in order to reply to you. Your inquiries are registered in the document management system of RIK and forwarded to the appropriate employees for reply. If we need to make further inquiries from someone else in order to respond to you, we will disclose your personal data only to the extent necessary for this purpose.

In accordance with the Public Information Act, the data set of your inquiry is visible in our [document register](#) [4]. For registered documents with a restriction on access, only the initials of the sender or recipient are visible from the public document register, not their name or the content of the

document.

If you have sent us an inquiry that falls within the competence of another authority, we will forward it to the appropriate authority. We will notify you of having forwarded the inquiry as well.

If someone wants to view your correspondence, a restriction on access means that upon receipt of an information request, we will review whether the requested document can be issued and whether it can be done in part or in full.

Irrespective of the restriction on access, we will issue the document to an authority or person who has a direct legal right to request it (e.g. investigative body, body conducting extra-judicial proceedings or court).

We may also use correspondence with you internally to evaluate the quality of our work.

Correspondence statistics and summaries are disclosed in an impersonal manner, without names.

Correspondence with private persons (requests for information / memoranda, etc.) will be stored for five years. After that period, the relevant documents are destroyed.

2.5.1 Contacting helpdesk

Calls received by the RIK helpdesk (+372 680 3160) are recorded and the caller is notified of this at the beginning of the call. The recordings will be used for improving service provision and these will be stored in a non-personal data format for at least six months. Recordings are automatically destroyed by the recording system after a certain period of time.

If you do not want to be recorded, you can opt out of the call and choose another way to receive the information (e.g. by email or regular post).

2.6.1 Visiting the Centre of Registers and Information Systems

When arriving for a meeting at RIK, visitors entering the building are first welcomed by a member of the security team working at the visitor entrance, who has previously been given the name of the person visiting the building. The member of the security team has the right to ask for your identity document to establish your identity. The visitor is provided with a visitor card, which gives the visitor access to the second floor, where the meeting rooms of RIK are located. The visitor can move around the building when accompanied by the person he or she has come to meet.

There is 24-hour video surveillance inside and around RIK. The movement of persons in the building and on the premises (parking lots, adjacent areas) is recorded for security reasons.

Video recordings and door card logs are managed by USS Security Eesti AS. The recordings are stored for 30 calendar days and door card logs for one year.

2.7.1 If your data has been entered into the accounting software e-Financials (we act as the controller of the database)

Objective

The e-Financials is a web-based accounting software that helps entrepreneurs conveniently manage their accounting tasks. The software is located on the Company Registration Portal of the e-Business Register and can be used by the entrepreneurs themselves or their authorised persons (such as accountants). The e-Financials is aimed primarily at start-ups and small businesses, but also at non-profit associations and foundations.

The software consists of five main parts: modules for invoicing, accounting, reporting, personnel and settings, and the entire environment can be used both in Estonian and English.

Legal basis

Use of the software requires the conclusion of a monthly contract. The contract between the legal person and RIK is digitally signed in the e-Financials environment of the Company Registration Portal.

Storage period

The Client has the right to add unlimited amounts of data to the e-Financials during the validity

period of the contract for use of e-Financials. At the end of the contract period, the Client will be offered an archiving service. RIK shall store the Client's data in the archive of the e-Financials for seven years of the date of entering the data in the e-Financials.

If the Client does not want to store the data, RIK may delete the data seven years after it was entered.

Access to the e-Financials

According to the terms and conditions of the contract concluded between RIK and the Client, we ensure the confidentiality of information concerning the e-Financials that is not publicly available. The obligation of confidentiality shall apply for an unlimited period to all persons and bodies (including state authorities).

As a representative of the Client, a natural person who has been designated by the Client as a user with the right to use the e-Financials shall be entitled to use the e-Financials on behalf and at the expense of the Client.

Upon conclusion of the contract for use of the e-Financials, all members of the management board shall have the rights to use the e-Financials. The members of the management board can add more users and manage their rights. The Client shall be responsible for all Users acting on its behalf and shall ensure that any User acting on behalf of the Client shall comply with the terms and conditions of the contract for use of the e-Financials, as well as legislation and the requirements for using the e-Financials established by RIK.

RIK is the controller with regard to hosting, maintaining and developing the database. Therefore, the data is accessed by those RIK employees who have a direct need arising from their duties (including technical support for the database) to do so.

[More information about the e-Financials](#) [5]

3. Accessing the data concerning yourself

You have the following rights:

- to access the data that RIK has collected concerning you;
- to request the rectification or completion of inaccurate or insufficient personal data;
- to request the deletion of personal data for the use of which RIK has no legal basis;
- to request that the processing of your personal data be restricted (e.g. for the time that the accuracy of your personal data is verified);
- to object to the processing of your personal data.

To this end, you can send an inquiry to us by using the [inquiry form](#) [6].

NB: In order to access personal data concerning yourself in the databases maintained by RIK, please contact the controller of the database. However, if you do send your inquiry to RIK, we will forward your inquiry to the controller of the database and will notify you of having done so.

We will respond to your inquiry as soon as possible, but no later than one month of receiving the inquiry. If data cannot be issued within one month, we will notify you thereof and extend the term for replying. We can issue data collected about you on paper or electronically, as requested. If there is reasonable doubt concerning the identity of the person making the request, we may require additional information to identify the person making the request.

If you want to receive data in paper format, we will charge a reproduction fee of 0.19 euros per page starting from page 21 in accordance with subsection 25 (2) of the [Public Information Act](#) [7]. If the request is unjustified or excessive (particularly due to its repetitive character), RIK has the right to charge a reasonable fee for the execution of the request or to refuse to issue the requested data.

3.1. We refuse to fulfil your access request if it may:

- adversely affect your rights and freedoms;
- hamper the prevention of a criminal offence or the apprehension of a criminal offender;
- complicate the ascertaining of the truth in criminal proceedings;
- threaten the protection of the confidentiality of a child's filiation.

You have the right to submit a complaint challenging our decisions to the Data Protection Inspectorate or file an application with [an administrative court](#) [8].

4. Infringement related to the processing of personal data

Should an incident involving an infringement of personal data processing occur in RIK, we will record the incident and prepare the required documentation.

If the incident is a potential threat to your rights and freedoms, we will inform the Data Protection Inspectorate. You can read more about infringements that are likely to threaten your rights and freedoms from the Data Protection Inspectorate's [General Guidelines for Personal Data Processing](#) [9].

If the infringement is likely to threaten your rights and freedoms, we will also notify you of the incident, so that you can take appropriate precautionary measures to mitigate the situation. If the infringement has occurred or is still ongoing at the time of discovery, we will take all necessary measures to end the infringement and mitigate its consequences.

5. Contact details

These data protection conditions have been prepared by Sirli King-Peets, Data Protection Officer of RIK. If you have any questions related to the processing of your personal data by the Centre of Registers and Information Systems, please contact our Data Protection Officer by sending an email to Sirli.King-Peets@rik.ee [10].

Source URL: <https://www.rik.ee/en/agency/data-protection-conditions>

Links:

[1] <http://www.privacy-regulation.eu/et/12.htm>

[2] <https://www.riigiteataja.ee/akt/129062018016?leiaKehtiv>

[3] <https://www.rik.ee/et/asutusest/toopakumised>

[4] <https://www.rik.ee/et/asutusest/dokumendiregister>

[5] <https://www.rik.ee/en/e-financials>

[6] <https://www.rik.ee/et/form/poordumine>

[7] <https://www.riigiteataja.ee/akt/122032011010?leiaKehtiv>

[8] <https://www.kohus.ee/>

[9] https://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/2019%20juhised/Isikuandmete%20tootleja%20uldjuhend.pdf

[10] Sirli.King-Peets@rik.ee?subject=Andmekaitsetingimused