

GENERAL PRIVACY POLICY OF THE EESTI APP MOBILE APPLICATION

What belongs in the scope of this privacy policy?

This privacy policy (**privacy policy**) describes the processing of personal data in the Eesti app mobile application. The privacy policy covers the processing of personal data in the Eesti app mobile application by the Information System Authority (RIA/we/us):

- regarding a user who has logged into the mobile application; and
- regarding services provided by RIA - authentication services, online services (enquiries in the self-service), mailbox, and other services listed in the privacy policy.

We also inform you about your rights regarding your personal data through the privacy policy.

What is not covered by this privacy policy?

Other processing conducted by RIA outside the Eesti app mobile application is described on the website of RIA at <https://www.ria.ee/en/authority-news-and-contact/processing-personal-data#website-phonenummer>.

Why read the privacy policy?

You should read the privacy policy because it contains important information about the processing of your personal data and describes your rights regarding personal data.

Where can I find additional information?

If you need additional information or have any questions about the processing of your personal data in the Eesti app mobile application, please contact us using contact details provided in subsection 3.1.

1. STRUCTURE OF THE PRIVACY POLICY

1.	STRUCTURE OF THE PRIVACY POLICY	1
2.	DEFINITIONS	2
3.	GENERAL INFORMATION AND CONTACT DETAILS	2
4.	CATEGORIES OF DATA SUBJECTS	3
5.	GENERAL PURPOSES, BASES, AND OPERATIONS OF PROCESSING	4
6.	EESTI APP MOBILE APPLICATION	5
7.	AUTHENTICATION SERVICES	7
8.	E-SERVICES	8
9.	NATIONAL MAILBOX	8
10.	DATA TRACKER, DATA CONSENT SERVICE, AUTHORISATIONS	10
11.	FORWARDING PERSONAL DATA AND PROCESSING BY DATA PROCESSORS	11
12.	SECURITY AND PRINCIPLES OF PERSONAL DATA	11
13.	RIGHTS OF DATA SUBJECTS PURSUANT TO THE GENERAL DATA PROTECTION REGULATION ..	13
14.	PERSONAL DATA OF CHILDREN AND REPRESENTATIVES AND EMPLOYEES OF SERVICE PROVIDERS	

15.	AMENDMENTS	14
-----	------------------	----

2. DEFINITIONS

- 2.1. The concepts of the protection of personal data are used in the meaning defined herein or in the [General Data Protection Regulation \(2016/679\) \(GDPR\)](#). To help with reviewing the text, we have explained some concepts of the GDPR in this chapter; however, we use the basic terminology of the GDPR in lowercase throughout the main body of the privacy policy.
- 2.2. **Data subject/you** - a natural person, regarding whom we have information that can be used for the identification of the natural person.
- 2.3. **Self-service** - the view of the user when logged into the state portal eesti.ee. A data subject is able to use the services in the self-service.
- 2.4. **Cookies** - data files that are stored in the devices of the visitors of the state portal eesti.ee based on the choices made by the visitors regarding cookies. Additional information about the use of cookies is available on the eesti.ee website in the cookies solution and in the Cookie Policy.
- 2.5. **Eesti app mobile application** - mobile application based on the state portal eesti.ee that only functions when logged in and entails the most commonly used services displayed in the state portal eesti.ee.
- 2.6. **Privacy policy** - this privacy policy describing the processing of personal data in the state portal eesti.ee.
- 2.7. **RIA/we/us** - the Estonian Information System Authority.
- 2.8. **Service provider** - usually, a legal person performing public law functions, whose services can be accessed via the state portal eesti.ee.
- 2.9. **Service(s)** - services, queries, etc. which can be accessed through the Eesti app mobile application and authentication services offered by RIA. To be more precise, *services* entails the following services:
 - a) **Data Tracker** - the Data Tracker functionality provided by RIA, which a data subject can use for reviewing the processing of their personal data in national databases;
 - b) **authentication services** - RIA provides the following authentication services: State Authentication Service (TARA); government SSO service (GovSSO); and the Estonian node of the cross-border authentication infrastructure of the European Union (National eIDAS-Node) (together, 'authentication services');
 - c) **e-services** - queries, requests, and linked information available through the self-service provided via X-tee;
 - d) **data consent service** - data consent service provided by RIA, which a data subject can use for granting access to their personal data in national databases to the state or a company for payment in instalments, for example;
 - e) **national mailbox service** - email account service using the address personalidentificationcode@eesti.ee (also, for the representatives of legal persons: registrycode@eesti.ee) that can be used by state authorities and other entities performing public duties for sending notifications and information that are forwarded to the email address (via email) or to the phone number (with a text message) selected by the data subject or RIA based on the data in the population register.

3. GENERAL INFORMATION AND CONTACT DETAILS

- 3.1. **About us.** Information System Authority (in Estonian: Riigi Infosüsteemi Amet, or **RIA**); commercial registry code: 70006317; address: Pärnu mnt 139a, Tallinn, Harju County 15169;

general email address: ria@ria.ee. The Information System Authority is a competence centre that designs and fortifies the basic pillars of the Estonian digital society - it develops and manages central technological platforms of the digital state and helps to ensure national cybersecurity.

- 3.2. **Contact details for data protection.** If you have any questions about the processing of personal data, feel free to email us at andmekaitse@ria.ee. You can contact our data protection officer by sending an email to andmekaitse@ria.ee or using the contact form at <https://www.eesti.ee/eraisik/en/vajad-abi>.
- 3.3. **About the privacy policy.** This privacy policy applies to the processing taking place in the Eesti app mobile application. It also covers the provision of services of the Eesti app mobile application by RIA. RIA may amend the privacy policy unilaterally. We inform the data subjects of all significant changes in the state portal or through other channels.
- 3.4. **About the status of the data controller and the data processor.** RIA performs various roles when processing personal data.
 - 3.4.1. To be more precise, RIA is the **data controller** in the processing operations that fall within the scope of the privacy policy in the following situations:
 - a) provision of the Data Tracker service;
 - b) in the mobile application;
 - c) provision of the data consent service;
 - d) provision of the national mailbox service;
 - e) logging user behaviour and the user journey in the entire Eesti app mobile application.
 - 3.4.2. RIA is a **data processor** in the processing operations that fall within the scope of the privacy policy in the following situations:
 - a) provision of the authentication service;
 - b) provision of the e-service functionality in the self-service (i.e. in respect to queries made through the self-service);
 - c) regarding the contents of the emails in the national mailbox;
 - d) when using IT services (where a service provided by a third party is used) or providing them in accordance with the instructions of the data controller.
- 3.5. **Other links/applications, etc.** Links in the mobile application may lead to websites where the privacy policies of the specific service providers are applied instead of this privacy policy. RIA is not liable for the content published on other websites or how they process personal data. Your personal data is processed in the social media channels of RIA pursuant to the privacy policy of the platform concerned, established by the providers of the platforms. RIA complies with the terms and conditions established on the platforms regarding the processing taking place on its social media platforms as well as this policy.

4. CATEGORIES OF DATA SUBJECTS

- 4.1. **Categories of data subjects.** Pursuant to the privacy policy, RIA processes the personal data of the following data subjects:
 - a) persons who have logged into the Eesti app mobile application (natural persons, representatives of legal persons who are natural persons);
 - b) officials and employees of RIA;
 - c) officials and employees of service providers (e.g. the name and email address of a representative of the Unemployment Insurance Fund);
 - d) other data subjects (e.g. regarding the content of the queries - wards, children, a spouse, a cohabitee, etc.);

e) the employees and officials of a source organisation of a query (e.g. information about a family physician in the Health Insurance Fund).

Employees of RIA are notified about the processing of their personal data internally. Information about the processing of the personal data of job applications is available in the privacy policy published on the website of RIA at <https://ria.ee/en/authority-news-and-contact/processing-personal-data#website-phonenummer>.

4.2. **Collection of personal data.** RIA receives personal data from service providers, third parties (e.g. the sender of an email in the case of the mailbox), or the data subjects themselves. Usually, data processing takes place through X-tee.

5. GENERAL PURPOSES, BASES, AND OPERATIONS OF PROCESSING

5.1. **Consent.** Based on consent, RIA processes personal data precisely within the limits, to the extent, and for the purposes to which the data subject has consented. We consider the consent of a data subject valid where it has been given freely, is specific, informed, and unambiguous (such as checking a box on a website). The data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of the processing conducted under the consent prior to the withdrawal.

5.2. **Conclusion and performance of an agreement.** When RIA concludes an agreement with a data subject, the processing of personal data required for the performance of the agreement takes place based on the agreement and within its scope.

5.3. **Public interest.** RIA allows access to the mobile application and provides services in the course of performing its public law functions, and therefore, the main basis for the processing of personal data is public interest ([Article 6 \(1\) e\) of the GDPR](#)).

5.4. **Legal obligation.** RIA may rely on the law as a basis for processing when the respective obligation has been specifically established by the law. For example, RIA may process personal data pursuant to the law to perform obligations stipulated in section 32¹ of the Public Information Act and in implementing legislation.

5.5. **Legitimate interest.** When performing its public law functions, RIA does not rely on legitimate interest as a basis for processing. Legitimate interest may be relied on when RIA processes data for other purposes (partnerships due to public law functions, professional relationships, etc.). Where RIA relies on legitimate interest, we have already assessed our interests and those of the data subject and analysed the justification of the processing thoroughly. The data subject is entitled to review the assessment of the processing of their personal data by contacting us using the details in subsection 3.2. RIA may process the personal data of a data subject (except for special categories of personal data and when performing public law functions) based on legitimate interest for the following purposes:

5.5.1. ensuring a better user experience;

5.5.2. conducting satisfaction surveys and measuring the efficiency of marketing activities;

5.5.3. preparing, submitting, or justifying legal requirements.

5.6. **New purpose.** Where personal data is processed for other purposes than the original objective of collecting it or when it is not based on the consent of the data subject, we carefully assess the permissibility of such new processing. In order to determine whether the processing for the fulfilment of a new purpose complies with the original purpose of the collection of personal data, we take into consideration, among all else, the following:

5.6.1. any connection between the purposes of the collection of personal data and the purposes for which the data is further processed;

5.6.2. context of the collection of personal data - primarily regarding the relationship between the data subject and us;

5.6.3. nature of the personal data - primarily whether the processing concerns any special categories of personal data or personal data related to convictions and offences;

- 5.6.4. possible consequences of the further processing for the data subjects;
- 5.6.5. existence of relevant protective measures that may include encryptions or pseudonymisation.

6. EESTI APP MOBILE APPLICATION

- 6.1. **Roles in processing.** RIA is the data controller of the Eesti app mobile application. In the case of persons who have logged in, RIA’s role in processing depends on the specific service.
- 6.2. **Objectives of processing.** RIA is a data controller in the Eesti app mobile application when processing data for the following purposes:
 - 6.2.1. allowing access to the application, which includes:
 - a) development and analytics;
 - b) ensuring security;
 - c) access to the Eesti app mobile application - login;
 - d) forwarding data through feedback, contact, and other forms;
 - e) notifications that contain national threat alerts as well as notifications to your national mailbox.
 - 6.2.2. Services which are made available through the mobile application and the processing of personal data during the provision of the services by RIA are described in the subsequent chapters.
- 6.3. Information regarding the processing of personal data in the Eesti app mobile application (purpose, basis, personal data, retention):

PURPOSE	BASIS	PERSONAL DATA	RETENTION
Allowing access to the mobile application	Article 6 (1) e) of the GDPR - public interest for allowing access to public services (information gateway) (section 32 ¹ of the Public Information Act and the Information Gateway Regulation - see subsection 32 ¹ (5) of the Public Information Act; statutes of the Information System Authority) and an obligation established by law in the extent of the mandatory processing in accordance with the law.	Technical information (including device details, IP address, application traffic - logs). Information submitted through the feedback and contact forms.	Logs are stored for up to 5 years (workload logs are stored for 2 years, for example). Information provided through forms; feedback is stored for up to 3 years in the case of the contact form and up to 3 years in case of the feedback form.
Development and analytics of the mobile application	Article 6 (1) e) of the GDPR - public interest for allowing access to public services (information gateway) (section 32 ¹ of the Public Information Act and the Information	See the previous row.	Cookies are stored pursuant to the cookie policy mentioned in the cookie solution. Logs are stored for up to 5 years (workload

	<p>Gateway Regulation - see subsection 32¹ (5) of the Public Information Act;</p> <p>statutes of the Information System Authority) and an obligation established by law in the extent of the mandatory processing in accordance with the law.</p> <p>Legitimate interest of asking for feedback to the functioning of the website (Article 6 (1) f) of the GDPR).</p>		<p>logs are stored for 2 years, for example).</p> <p>Information provided through forms; feedback is stored for up to 3 years in the case of the contact form and up 3 years in case of the feedback form.</p> <p>Other information based on the objective of the collection.</p>
<p>Logging into the mobile application, authentication</p>	<p>Article 6 (1) e) of the GDPR - public interest for allowing access to public services (information gateway) (section 32¹ of the Public Information Act and the Information Gateway Regulation - see subsection 32¹ (5) of the Public Information Act;</p> <p>statutes of the Information System Authority) and an obligation established by law in the extent of the mandatory processing in accordance with the law.</p>	<p>Full name, personal identification code, authentication details, technical information regarding traffic in the information gateway, logs.</p>	<p>Login data is stored for 18 months.</p> <p>Logs are stored up to 5 years, depending on the manner selected for logging in.</p> <p>Other information based on the objective of the collection.</p>
<p>Ensuring security</p>	<p>Legal obligation (Public Information Act and the Information Gateway Regulation; statues of the Information System Authority) and public interest.</p>	<p>Usually, technical information and logs; however, all personal data processed in the mobile application may be processed for ensuring security where necessary.</p>	<p>Logs are stored for up to 5 years (workload logs are stored for 2 years, for example).</p> <p>Other information based on the objective of the collection.</p>
<p>Push notifications for ensuring safety and informing the users</p>	<p>Article 6 (1) e) of the GDPR – public interest regarding the performance of legal obligations and ensuring security.</p>	<p>Full name, personal identification code, data.</p>	<p>Logs are stored for up to 5 years (workload logs are stored for 2 years, for example).</p>

7. AUTHENTICATION SERVICES

- 7.1. **Roles in processing.** When providing authentication services, RIA is a data processor when it allows access to the services of another authority/service provider. In this case, the authority/service provider whose services are being accessed is the data controller and RIA processes data relying on the bases of the data controller. RIA is the data controller when it comes to the development, security, and logs of the authentication service.
- 7.2. **Purposes of processing.** The purposes of data processing conducted by RIA are allowing the use of the authentication services, meeting the related public interest, and ensuring security.
- 7.3. When providing authentication services, only the selected trust service provider authenticates the person. RIA does not use sub-processors for providing the authentication services.
- 7.4. **For a more thorough description** of the authentication services, please click on this link: <https://www.ria.ee/en/state-information-system/electronic-identity-eid-and-trust-services/central-authentication-services>.
- 7.5. RIA as a data controller - information regarding processing during the provision of the authentication services (purpose, basis, personal data, retention):

PURPOSE	BASIS	PERSONAL DATA	RETENTION
Development and analytics of the service	Article 6 (1) e) of the GDPR - public interest.	Usually, de-identified data, but where necessary, authentication data may be processed - i.e. the following data is processed when providing the authentication services: data that can be used for the identification of the user (in other words, the natural person using the authentication service): authentication certificate, personal identification code or another personal identifier; first and last name; date of birth; country; mobile phone number; commercial registry code or another identifier of a legal person; business name of a legal person; selected language; as well as the data of the authentication process: date and time; application that directed the user to authentication; authentication method; IP address from which the user was directed to authentication; result of the authentication (authenticated or not).	The data is not stored separately, which means that data is stored pursuant to the original purpose of collecting it.
Ensuring security and logs	Legal obligation (Public Information Act and the Information Gateway Regulation; statues of the Information System Authority) and public interest.	Usually, technical information and logs; however, all personal data processed in the mobile application and the authentication service may be processed for ensuring security where necessary.	Logs are stored for 18 months. Other information based on the objective of the collection.

8. E-SERVICES

- 8.1. **Roles in processing.** RIA is a data processor when it comes to queries and requests of e-services and access to/linking information to e-services. As a data processor, RIA conducts processing operations on the same basis as the service provider that is the data controller.
- 8.2. **Purposes of processing.** Information about a service provider can be found by the query/request (name, contact details). For more information about the processing of personal data by a service provider, please review the website and privacy policy of the respective service provider.
- 8.3. Information forwarded to a service provider with an e-service query or request can be seen in the query/request. The query/request may be accompanied by technical information for checking and allowing the query/request. Information exchange between RIA and a database takes place in three ways in the case of e-services (individual queries):
- linking. Exchange of information through linking means that a reference to the location of the requested information in a database is made available in the Eesti app mobile application, whereas the information itself is not disclosed. In addition, information pertaining to personal data is not forwarded from the database to RIA in the case of linking and RIA does not forward information containing personal data to the database;
 - request. Exchange of information through a request means that an individual submits information containing personal data to the database through RIA to receive the selected service;
 - query. Exchange of information through a query means that information in databases is made available. In the case of a query, the database forwards information containing personal data to RIA.
- 8.4. **Further information** regarding e-services can be found in short descriptions accompanying specific e-services or on the websites of the service providers.
- 8.5. RIA is the data processor when facilitating e-services (individual queries) (see chapter 111) and does not use sub-processors.
- 8.6. RIA as a data processor - information regarding the processing of personal data in the course of providing e-services (purpose, basis, personal data, retention) is presented in the following table:

PURPOSE	BASIS	PERSONAL DATA	RETENTION
Services of the service providers in the Eesti app mobile application	Legal basis of the data controller	Information forwarded with a query or a request in the case of e-services to the service provider and made available in the Eesti app mobile application. The query/request may be accompanied by technical information for checking and allowing the query/request.	Pursuant to the privacy policy of the data controller.

9. NATIONAL MAILBOX

- 9.1. **Roles in processing.** RIA is the data controller in regard to the national mailbox service.

- 9.2. The national mailbox service can only be accessed by a data subject who has logged in. Therefore, processing is preceded by authentication when logging into the mobile application (for more details, see chapter 7).
- 9.3. **Purposes of processing.** The general purpose of the national mailbox service is to provide state authorities and other parties performing public duties with the function of sending notifications to data subjects through their email address personalidentificationcode@eesti.ee or to the representatives of legal persons through registrycode@eesti.ee; however, this purpose is accompanied by and it is related to ensuring security as well as development and analytics. The national mailbox cannot be used for sending emails; i.e. emails can only be received and forwarded to the email address selected by the data subject.
- 9.4. RIA as the data controller - information on the processing of personal data in the national mailbox service (purpose, basis, personal data, retention):

PURPOSE	BASIS	PERSONAL DATA	RETENTION
Allowing the use of the eesti.ee mailbox	Article 6 (1) e) of the GDPR - public interest regarding the provision of public services (section 32 ¹ of the Public Information Act and the Information Gateway Regulation - see subsection 32 ¹ (5) of the Public Information Act; statues of the Information System Authority).	Email address, personal identification code, phone number, and the content of notifications of the data subject. RIA is not the data processor in regard to the content of the notifications and emails.	As a rule, the notifications are stored for at least 3 years, except for when the data subject deletes the information before that, the sender of a notification recalls the notification, or the sender of a notification has set a specific retention period.
Forwarding to another email address and/or enabling the forwarding of a notification to a phone	Consent through action - a data subject enters their preferred email address and/or phone number. Article 6 (1) c) of the GDPR - legal obligation - on this basis, RIA and the population register update their data (for example, section 53 of the Regulation on the Structure of the Population Register, Security Class, Exact Data Composition, and List of Data to be Transferred by Data Providers, based on which RIA provides the forwarded official email address with its start and end date and the person's phone number).	Email address and phone number of the data subject and the content of notifications. RIA is not the data processor in regard to the content of the notifications and emails.	The data subject can change the email address and phone number that they have added.

Development and analytics of the service	Article 6 (1) e) of the GDPR - public interest regarding the provision of public services (section 32 ¹ of the Public Information Act and the Information Gateway Regulation - see subsection 32 ¹ (5) of the Public Information Act; statues of the Information System Authority) and an obligation established by law in the extent of the mandatory processing in accordance with the law.	Full name, personal identification code, authentication details, technical information about traffic in the mobile application, information about the use of the mailbox service, logs.	Logs are stored for up to 5 years (workload logs are stored for 2 years, for example). Other information based on the objective of the collection.
Ensuring security	Legal obligation (Public Information Act and the Information Gateway Regulation; statues of the Information System Authority) and public interest.	Usually, technical information and logs; however, all personal data processed in the mobile application may be processed for ensuring security where necessary.	Logs are stored for up to 5 years (workload logs are stored for 2 years, for example). Other information based on the objective of the collection.

9.5. **Please note that forwarding messages from the national mailbox comes with risks.** RIA wishes to draw your attention to the fact that, in the course of forwarding messages, the notifications and personal data contained therein (if applicable) may be sent outside the European Economic Area (EEA) depending on the provider of the email or communication service chosen by the data subject, and as a result of the forwarding, the content (and personal data) of the emails may also come to the possession of service providers with questionable security, in which case the completeness and confidentiality of your emails and their content is not guaranteed.

In certain instances, RIA adds an email address or a phone number for forwarding as a result of its own operations (such as voter information before elections and information exchange with the population register).

9.6. RIA uses the Estonian Government Cloud service of the Estonian IT Centre as a data processor when providing the mailbox service.

10. DATA TRACKER, DATA CONSENT SERVICE, AUTHORISATIONS

10.1. Data Tracker.

10.1.1. You can use the Data Tracker to find out about the processing of your personal data in national databases. The Data Tracker displays queries pertaining to you, including those where personal data has been requested by a third party. RIA is the data controller when providing the Data Tracker service. The privacy policy of the Data Tracker contains information about the processed personal data, purposes, and bases.

10.1.2. For more information about the Data Tracker, please review the service description at [RIA - Data Tracker](#).

10.2. Data consent service.

- 10.2.1. A data subject may use the data consent service to allow companies to access their personal data in national databases. Consent can only be given for the transfer of the data set required for a specific service, following which the data held by the state is forwarded to the selected private enterprise. By using the data consent service, a data subject may exercise their legal right to decide on the processing of their personal data by choosing third parties who can access their data. The use of the data consent service and the giving of consent is always voluntary. Consent can be revoked at any time. The privacy policy of the data consent service contains information about the processed personal data, purposes, and bases.
- 10.2.2. For more information about the data consent service, please review the description of the service at [RIA - Data consent service](#).

11. FORWARDING PERSONAL DATA AND PROCESSING BY DATA PROCESSORS

- 11.1. **Use of partners.** RIA cooperates with parties to whom information regarding data subjects (including personal data) may be forwarded in the course of and for the purposes of a partnership. RIA may have various types of relationships with these partners as a data controller, data processor, or a sub-processor. Forwarding personal data to third parties takes place in strict compliance with the applicable data protection requirements.
- 11.2. **Requirements to the use of partners who are our data processors.** Among all else, such third parties may include:
- a) advertisement and marketing partners (data from cookies);
 - b) various consultants (depending on the service, information required for the provision of the service);
 - c) providers of state services, such as the server service provider - Estonian Government Cloud service provided by the Estonian IT Centre;
- provided that the relevant purpose and processing are legal and personal data is processed based on the instructions of the data controller and a valid agreement.
- In regard to partners and data processors, please use the contact details listed in subsection 3.1 for requesting additional information.
- 11.3. **Other forwarding.** In other instances, we may forward your personal data to third parties, provided that we have basis for such forwarding, such as your consent or a legal obligation. Generally, these parties are separate data controllers. Such parties may be:
- 11.3.1. auditors and legal advisers (depending on the service, all personal data may be forwarded);
- 11.3.2. state authorities and investigative authorities - in certain cases, we may be obligated to disclose your personal data when it is required by law or when public sector institutions submit a valid request to that effect. Before disclosing personal data, we always assess the legality of the requests for information; the disclosure of information may be necessary to protect or prove our rights or the rights of a third party.
- 11.4. **Forwarding outside the European Economic Area (EEA).** RIA processes personal data in the EEA. The data of a data subject may move outside the EEA if the data subject or RIA forwards emails from the national mailbox to an email provider outside the EEA (see subsection 9.55 above).

12. SECURITY AND PRINCIPLES OF PERSONAL DATA

- 12.1. **Security measures.** The security of personal data processed by RIA is ensured with organisational and technical measures. Among all else, we do the **following** to ensure security and confidentiality:

Measures concerning specific data that is processed

Encryption	All components of the information system use encryption. Traffic between the components is encrypted, components identify one another with certificates (HTTPS protocol, TLS).
Anonymisation	As a rule, RIA does not anonymise personal data. However, it does apply pseudonymisation; for example, the value of a cookie is stored in logs without a personal identification code.
Logical access control	Access is granted to employees of RIA based on need and accessing information requires a password (through Active Directory); moreover, there is no access outside the RIA network. The activities of the employees are logged based on usage, or in other words, the application logs the movements of the employee. In addition, restrictions on downloads and printing are applied to employees (as an organisational measure; i.e. it is prohibited without permission). Access to information stored in the Government Cloud of the Estonian IT Centre is additionally granted to people who are needed for managing the Government Cloud of the Estonian IT Centre.
Observability (logging)	The entire content of the mobile application is logged.
Archiving	The security control system of the Estonian Information Security Standard is used when storing data.

General security measures concerning systems where processing takes place

Security of availability	The servers that are used are managed by RIA or are virtual servers.
Website security	Unchecked developments in production are not implemented in the live environment. An independent provider of security testing checks new services and applications. Penetration testing is an obligatory stage before production for discovering security vulnerabilities. All websites are HTTPS. Protection against cyber attacks is provided by Cloudflare (managed by CERT) to protect the entire traffic (e.g. in the case of many attacks from a specific source, the source is blocked).

Organisational measures

Organisation	RIA employs a data protection officer. Access to the physical locations of RIA is highly regulated.
Policies, rules	Guidelines regarding data protection and information security have been prepared for officials and other employees.
Risk management	RIA has adopted a risk management guideline that is reviewed annually.
Incident and data breach management	In the case of incidents, instructions for the officials and employees regarding steps to be taken are included in the Data Protection Guideline.
HR management	RIA provides further training.

- 12.2. **Incident.** In the case of an incident related to personal data, RIA does its best to alleviate any consequences and reduce such risks in the future. RIA complies with the notification requirements of the General Data Protection Regulation.
- 12.3. **Compliance with requirements and purpose.** The purpose of RIA is to process personal data responsibly so that it is able to demonstrate compliance with the purposes of the processing of personal data and applicable law.

- 12.4. **Principles.** All processes, guidelines, and operations related to the processing of personal data conducted by RIA are based on the following principles: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and data protection by design and by default.

13. RIGHTS OF DATA SUBJECTS PURSUANT TO THE GENERAL DATA PROTECTION REGULATION

- 13.1. RIA wants to ensure that the data subjects are completely informed of all of their rights regarding personal data. The data subjects have the following rights when the requirements set out in the GDPR have been met:
- a) **Right of access to personal data** - the data subject has the right to access their personal data and to obtain a copy of the data.
 - b) **Right to rectification of data** - the data subject has the right to demand the rectification of inaccurate or incorrect data.
 - c) **Right to the erasure of data** - the data subject has the right to demand the erasure of personal data concerning them under certain conditions (for example, when we process your personal data based on your consent).
 - d) **Right to restrict the processing of personal data** - the data subject has the right to request the restriction of the processing of their personal data under certain conditions (for example, we process your personal data based on your consent or legitimate grounds).
 - e) **Right to object to the processing** - the data subject has the right to object to the processing of personal data concerning them under certain conditions (for example, when we process your personal data based on legitimate grounds).
 - f) **Right to data portability** - under certain conditions, the data subject has the right to require that personal data concerning them is transmitted to another organisation.
 - g) **Rights related to consent** - the data subject has a right to withdraw their consent at any time (for example, while logged into the eesti.ee dashboard, under consents). Withdrawal of consent does not change the legality of processing carried out before the withdrawal.
 - h) **Rights related to legitimate interest** - when RIA processes the personal data of a data subject based on legitimate interest, the data subject has the right to access the assessment of legitimate interest completed regarding the processing of their personal data.
 - i) **Rights related to automated processing and profiling** mean that the data subject, based on their individual circumstances, has the right to object to being subjected to a decision based on automated processing, including profiling, of their personal data at any time, and to request for human intervention if the aforementioned processing would produce legal effects concerning the data subject or have a similarly significant impact. The data subject may require for an explanation of the logic behind the automated decision. **In the interests of clarity: RIA may rely on automated processing or profiling in the course of processing that falls under the scope of the privacy policy, which affects the data subject or their rights significantly; for such cases, RIA has conducted an impact assessment which can be accessed by contacting us.**
 - j) **Right to lodge a complaint** - the data subject has the right to lodge a complaint with RIA or a supervisory authority or a court if the data subject believes that their rights in relation to the processing of personal data have been violated. **In order to resolve the issue, please contact us first.** If necessary, the contact details of RIA's supervisory authority (the Data Protection Inspectorate) regarding data protection are available here: <https://www.aki.ee/en/contact>. If you are a data subject of another EEA country, then you have the right to lodge a complaint with the supervisory authority of the country of your residence. The contact information of the data protection supervisory authorities of other EU countries is available [here](#).

- 13.2. **Replies and additional information.** RIA has one month to reply to requests related to the processing of personal data. Where justified, this deadline may be extended. If a data subject would like to exercise a right related to their personal data or needs additional information about their rights, then please email us using the contact details in subsection 3.1. RIA identifies the data subject before allowing them to exercise rights related to personal data to avoid the disclosure of personal data to the wrong person.
- 13.3. **The supervisory authority of RIA in respect to data processing** is the Estonian Data Protection Inspectorate <https://www.aki.ee/en>.

14. PERSONAL DATA OF CHILDREN AND REPRESENTATIVES AND EMPLOYEES OF SERVICE PROVIDERS

- 14.1. **The personal data of children** is processed based on public interest or due to a legal obligation when performing public duties.
- 14.2. The employees have been informed of the particularly sensitive nature of processing the personal data of children and the resulting stricter requirements through internal documents.
- 14.3. The basis for processing the data of a service provider in the course of performing a public duty is generally public interest and legal obligations (where the obligation to collect such data arose directly from the law). Under certain conditions, where the processing is outside the scope of public interest, the processing is based on legitimate interest (for example, when sending Christmas greetings to the representatives of partners).

15. AMENDMENTS

- 15.1. Past amendments and entry into force of the privacy policy:

Published	Entry into force	Main amendments
17 June 2025	17 June 2025	New name for the mobile application
13 October 2024	13 October 2024	Second version of the new privacy policy.
10 September 2024	10 September 2024	First version of the new privacy policy.