

Privacy Disclaimer

for processing of personal data in insurance portal

Citadele

Effective 01.07.2026

We, AS "Citadele banka" Estonian branch (registration number 11971924, registered address Narva mnt 63/1, 10120 Tallinn, Estonia, have developed this privacy disclaimer to provide you with information about what data we process, why and how we protect it when you use the insurance portal.

We provide this information in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council (27.04.2016) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, hereinafter - the Regulation, as well as in compliance with the legislation of the European Union and Estonia, recommendations and best practices of the financial sector and supervisory authorities.

The maintenance of the insurance portal and the processing of information on the insurance portal are carried out by us in cooperation with our Swedish cooperation partner Insurely AB (registration number 559103-5646). The insurance offer itself for you will be prepared by our insurance cooperation partner AAS BTA Baltic Insurance Company Estonian branch (registration number 11223507, registered address Lõõtsa tn 2b, 11415 Tallinn, Estonia). Personal data necessary for preparing an insurance offer, concluding an insurance contract and issuing an insurance policy may be transferred to this insurance partner.

This privacy disclaimer provides an insight into the personal data protection and processing conditions that Citadele complies with in relation to the processing of personal data carried out, including processing carried out in cooperation with Insurely AB.

If you would like to get acquainted with the personal data protection and processing conditions recognized by our insurance cooperation partner in relation to the processing of personal data carried out by it, we invite you to devote additional time and familiarize with the privacy protection conditions of AAS BTA Baltic Insurance Company Estonian branch. Further processing of personal data by AAS BTA Baltic Insurance Company Estonian branch is carried out in accordance with BTA's privacy policy. The privacy policy can be found [here](#).

Brief description of process (simply about the supposedly complicated) _____

Our insurance portal allows you to check the conditions of your current insurance policy and buy a new insurance policy from our insurance cooperation partner. You can buy a new insurance policy from our insurance cooperation partner even without checking the conditions of the current insurance policy.

The process of checking the conditions of your current insurance policy is simple. Namely, you connect to our insurance portal and, with the help of a secure connection, request the data of your current insurance policy from your current insurer. This data is sent to us to display key information about your existing insurance policy in the insurance portal and we pass only the data necessary for preparing a new insurance offer – such as information about the policyholder and the insured object – to our insurance cooperation partner. Consecutively, you can see on our insurance portal the key information about your current insurance policy and the conditions of a new insurance offer presented to you by our insurance cooperation partner. If you choose the offer of our insurance cooperation partner, you can immediately conclude a contract and receive the new insurance policy. This whole process is automated and safe and takes only a few moments.

The process of buying a new insurance policy is even simpler if you do not check the conditions of the current insurance policy – you provide us with the necessary data, we send it to our insurance cooperation partner so that it can prepare a new insurance offer for you, and after a moment you can already conclude a contract and receive a policy.

Who will process your data _____

AS "Citadele banka" Estonian branch (registration number 11971924, registered address Narva mnt 63/1, 10120 Tallinn, Estonia).

If you have any questions about data processing, you can contact us by calling +372 770 0000, writing to the e-mail address info@citadele.ee, or gdpr@citadele.ee reaching our appointed data protection officer.

Privacy Disclaimer

for processing of personal data in insurance portal

Citadele

For what purposes, what data, on what basis we process and how long we store it

Purpose of data processing	Data types/categories processed	Legal bases for processing	Data retention period
Obtaining data from you as a user of the insurance portal and transferring the collected data to our insurance cooperation partner for concluding a new insurance contract and issuing a new insurance policy.	Name, surname Personal ID code Date of birth Place of residence E-mail address Phone number	The processing is necessary for the performance of a contract (i.e. Terms for the verification and purchase of insurance) to which the data subject is a party.	18 months after the conclusion of the insurance contract. The data storage period will be extended every time you conclude a new insurance contract.
Obtaining up-to-date insurance information from your existing insurer for the preparation of a new insurance offer.	Name, surname Personal ID code Date of birth Place of residence E-mail address Phone number Data from the existing insurance policy	The processing is necessary for the performance of a contract (i.e. Terms for the verification and purchase of insurance) to which the data subject is a party.	18 months after retrieval of data from the existing insurer.
Transfer of data obtained from insurance cooperation partner regarding insurance offer to you.	Vehicle make and model Driver age group Years of driving experience Insurance premium amount End date of existing Motor Third Party Liability insurance (if applicable)	The processing is necessary for the performance of a contract (i.e. Terms for the verification and purchase of insurance) to which the data subject is a party.	Data is stored 14 to 30 days
Transfer of data obtained from your existing insurer to the insurance cooperation partner for the calculation of a new insurance offer.	Name, surname Personal ID code Date of birth Place of residence E-mail address Phone number Data from the existing insurance policy necessary to insurance offer calculation (policyholder and insured object data).	The processing is necessary for the performance of a contract (i.e. Terms for the verification and purchase of insurance) to which the data subject is a party.	Not applicable to this purpose, as the data is transferred to the insurance cooperation partner.
Maintenance of the insurance portal, the development of its functionality and data exchange process	All personal data to be processed within the framework of the service, if it is necessary for the achievement of the relevant purpose.	Citadele's legitimate interest in providing customers with quality services	No more than 18 months from the moment of obtaining the data.

Receipt information on you as a user of the insurance portal and applicant for insurance via email from Insurely AB and BTA to perform further actions related to assistance in using insurance portal, purchasing insurance or renewing if it has expired.	a) Name, surname Personal ID code Date of birth Place of residence E-mail address Phone number b) Name, surname Personal ID code Date of birth Place of residence E-mail address Data from the existing insurance policy (start/end date, policy number, object etc).	Citadele's legitimate interest in managing and improving the customer experience by: (a) identifying users who have not completed an insurance purchase, as well as (b) proactively communicating with customers, for example by sending reminders about the approaching expiry of a policy or offers to renew a policy.	18 months after the moment of entering an insurance contract or obtaining data.
Communicating with you as a user of the insurance portal and/or a customer regarding assistance in purchasing or renewing insurance after its expiration date.	Name, surname Personal ID code Place of residence E-mail address Phone number Data of the object of insurance and/or the terms of the existing and new policy Communication data	Communication and related processing of your personal data in cases of pending purchases is based on the performance of contracts (i.e. Terms for the verification and purchase of insurance) to which the data subject is a party.	18 months from the moment of receipt of the data.
		Communication in cases of insurance policy renewal and related processing of personal data is based on Citadele's legitimate interests (i) to improve the customer experience and reliability of our services, as well as (ii) to promote the sale of insurance policies.	18 months after the conclusion of the insurance contract. The data storage period will be extended every time you conclude a new insurance contract.
Handling of applications/claims related to the processing of personal data for the above-mentioned purposes.	All personal data processed within the framework of this process, as well as those personal data necessary for the examination of applications/claims.	Legitimate interest in responding to submissions, as well as resolving disputes arising in connection with maintaining a secure payment profile.	5 years from the date of examination of the application/claim or the date of final settlement in the relevant case.

Privacy Disclaimer

for processing of personal data in insurance portal

Citadele

Who we share your data with _____

Your data will be processed for the above purposes by authorized Citadele employees and employees of our cooperation partner Insurely AB. Please note that the insurance checking and purchase process is automated and does not require employee participation, so employees of our cooperation partner Insurely AB would be able to access your personal data only in the event of a failure in the operation of the insurance portal, the elimination of which would require their participation.

Your personal data necessary for preparing an insurance offer, concluding an insurance contract and issuing an insurance policy will be transferred to our insurance cooperation partner AAS BTA Baltic Insurance Company Estonian branch.

Citadele will not process your personal data outside the European Union or the European Economic Area.

What are your rights regarding the data processing we perform _____

Access your data	You have the right to receive from us: • confirmation of whether we process your data, • detailed information about your data processing to ensure that the data is accurate and processed in accordance with the law. If you wish to access your data, please specify the time and the data you want to receive. You have the right to know what data we hold about you, why we process it, how we obtained it, to whom it has been disclosed, and how long it will be stored. You may also request a copy of your data. To help us process your request more quickly, please specify the shortest possible time and describe precisely which data and information you wish to obtain. Please note that we may not be able to provide information if prohibited by law, for example, when data is shared with law enforcement authorities (police, prosecutor's office, court, etc.).
Correct data	If you believe that the data we hold is inaccurate or incomplete, please let us know: • specify the corrections needed, • we may request documents to verify the necessary changes.
Delete data	You may request the deletion of your data if you believe that: • it is no longer necessary, • it is not being used for its intended purposes. We will also delete your data from our cooperation partners unless it is necessary for the purposes for which it was processed or if the law requires a longer retention period. Please note that fulfilling a deletion request may not always be possible, for example if the data is needed to comply with legal requirements or for proceedings.
Restrict data processing	You may request to restrict the processing of your data if: • You contest the accuracy of the data (the restriction will apply until the accuracy is verified). • You believe the processing is unlawful but prefer to restrict rather than delete the data. • We no longer need your data, but you require it to exercise or defend your legal rights. • You object to data processing based on our legitimate interests. We will reassess whether, considering your objection, we need to continue processing your data. If data processing is restricted, we will only use the data for specific purposes, such as defending protecting our legal rights.
Transfer data	The data provided by you, either with your consent or under a contract, may be transferred. Data processed automatically can also be transferred. You can use this data personally, or,

	upon your request, we will transfer it to another service provider, provided there are no obstacles. When transferring data, it is important to consider that it may include third-party information. The transfer of such data must be carefully evaluated with respect to the rights and freedoms of those third parties. To speed up the request, please specify the exact data and information you wish to transfer.
Object to data processing	You may object to the processing of your data if it is conducted based on legitimate interests. We will review your objections and assess the necessity of continuing the data processing. We will need to continue processing your data if it is necessary to comply with the law or to protect our legal rights. You will not be able to exercise the right to object to the processing of your data if you have given your consent to the data processing, if data processing is necessary for the performance of a contract, or if we are required to process the data to comply with the law. Where processing is based on your consent, you have the right to withdraw that consent at any time. Withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

How to submit a request regarding data processing and how we will ensure the request is handled

When processing your data, we ensure that you have the following rights, which can be exercised by submitting a written request in free form:

How can you submit a request?	What will be the deadline for reviewing the request?	What will be the fee for reviewing the request?	How will we provide a response to the request?
In writing, in free form: - in person – by visiting the bank and presenting an identity document (passport or ID card), or a power of attorney if acting on behalf of someone else, - by email – by sending a request signed with a secure electronic signature, - via online banking. - through the mobile app.	We will review your request: - no later than within 1 month from the date of receipt, - if the request is extensive or complex, we may need an additional 2 months. We will inform you about the extension and the reasons for it.	You can receive a response to your request: - free of charge, - if you submit a repeated request and we determine that it is unfounded or excessive, we may apply a fee or refuse to fulfil the request. The fee will cover the costs of processing the information and the work of our employees. If a fee is required, we will inform you in advance.	You can receive a response to your request: - in person, by visiting the bank and presenting an identity document (passport or ID card), or a power of attorney if acting on behalf of someone else, - via email, by receiving a password sent via SMS to access the document, - through online banking, - via the mobile app.

How we protect your data

We ensure the protection of your data against unlawful access, use, disclosure by taking the following measures:
We restrict access to the premises to unauthorized persons by ensuring:

- Door locks (electronic doors): We make sure that all premises are locked if there are no employees in them.
- Access control: We use access cards (magnetic, chip cards), identity readers, code systems to control who can access the premises.
- Video surveillance, alarms, sensors: We install video surveillance cameras to monitor important premises and places.
- Selection of personnel: We select reliable employees.

We limit access to technological resources, ensuring:

- Protection of technological devices (computer devices (desktop computers, laptops, tablets, servers), mobile devices (smartphones), communication devices (routers, modems), data storage devices (external hard drives, flash drives, SD cards), other devices (printers, scanners, monitors, video cameras etc.).
- Protection of information systems, software, applications, and mobile applications.
- The protection of communication networks and technologies enables data transmission and information exchange (internet, VPNs, mobile networks, cloud technologies, etc.).

For the protection of technological resources, we provide:

- Prevention of environmental hazards: We implement safety measures against fires, floods, large temperature changes and other conditions.
- Prevention of technical risks: We take care that there is a good power supply, uninterrupted power supplies in case of power failures and that other similar malfunctions do not occur.
- Prevention of man-made hazards: We do not allow damage or theft.
- Secure passwords: We use secure and complex passwords for devices and accounts.
- Multi-factor authentication: We add an additional layer of security.
- Screen lock: When the device is not in use, we lock the screen.
- User roles: We limit access to data and systems, allowing only what is necessary for the relevant user.
- Software and security updates: We always install the latest versions to prevent vulnerabilities.
- Encryption: We encrypt data so that it cannot be accessed by third parties/unauthorized persons.
- Secure connection: We use HTTPS and VPN to ensure security when working online.
- Antivirus: We install and update antivirus programs on all devices.
- Firewalls: We use a firewall to protect the network from unwanted access.
- Attack detection systems: We install programs that monitor and warn about suspicious activity.

We carry out regular inspections and provide updates

- Equipment inspection: We regularly check that all devices are in working order and in place.
- System updates: We install the latest software updates to address security risks.

We educate employees

- Threat prevention: We warn you about fraudulent emails and other potential security risks.
- Training: We regularly inform employees about safety issues and how to act in suspicious situations.

We monitor and analyze security

- Log files (audit trails): We record access and operations in systems so that they can be monitored and reviewed.
- Regular tests: We check the safety of systems to identify and eliminate potential risks.
- We are ready for emergencies
- Backups: We regularly make backups of data and store them in safe places.

Emergency plan: We prepare a plan for what to do in case of a threat to premises or technology. Why is it important to us and to you?

Protecting technological resources helps protect data, prevent data leaks, theft, and guarantees that we can continue to work and avoid loss of money and reputation. Safety depends on each employee, so it is important to be careful and follow the rules.

Your data can only be accessed by us, Citadele Group employees, and cooperation partners who need it to perform their work duties. Before starting cooperation, we carefully evaluate the cooperation partners and inform them about the confidentiality and protection of data. We, Citadele Group companies and our cooperation partners, ensure the protection and use of your data only for the intended purposes, in accordance with the requirements of the law.

Privacy Disclaimer

for processing of personal data in insurance portal

Citadele

What should you do if you think your data rights have been violated _____

We process your data in accordance with regulations, European Union and Estonian laws, financial industry recommendations, and best practice guidelines. If you believe we have violated your privacy rights, you have the right to file a complaint:

AS "Citadele banka" Estonian branch Narva mnt 63/1, 10120 Tallinn Phone: +372 770 0000 Email: info@citadele.ee Data Protection Officer's email: gdpr@citadele.ee	Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon) Address: Tatari 39, 10134 Tallinn, Estonia Email: info@aki.ee Phone: +372 627 4135 Website: https://www.aki.ee
---	--

How will we ensure up-to-date information about the processing of your data _____

To ensure you are always informed about how your data is being processed, we regularly review and update this privacy notice. Therefore, we encourage you to periodically check the latest privacy notice on our website. If there are significant changes, we will notify you one month before they come into effect.