

Privacy Policy

Last modified on: September 1, 2022

Elbax OU ('we', 'Company', 'us') is the owner of the **Repost** mobile application placed on the App Store ('App', 'Services') and is committed to being fully transparent while operating it, as regards our privacy practices.

We developed this Privacy Policy to inform you ('you' or 'user') how your personal data may be processed. We tried to write this Privacy Policy in clear and plain language for your better understanding of the complicated legal stuff. By doing so we hope you will get all needed details to be assured your personal data is safe with us.

The Privacy Policy defines:

- what personal data we process;
- what are the purposes of such processing;
- what rights the user has concerning such data;
- whether the data is transferred to third parties;
- what measures we take to protect personal data;
- as well as other details of personal data processing.

This Privacy Policy is an integral part of our [Terms of Use](#). Please make sure you read them carefully.

If you have any questions about the Privacy Policy, the processing of your personal data by the Company, or the exercise of your rights as a personal data subject, send us a request to support@rpstservice.com.

1. What is Personal Data?

Personal data (or **data**) is any information relating to you, and that alone or in combination with other pieces of information allows the person who collects and processes such information to identify you as an individual. In general, these could be your name, email-address, location data etc. Personal data could also include such technical information as a Media Access Control address (MAC-addresses), International Mobile Equipment Identity (IMEI), Unique Device Identifier (UDID), the Identity for Advertisers (IDFA), Internet Protocol address (IP-address, both static and dynamic), browser, and system information.

Personal data processing means any action with it, for example, collection, recording, organizing, structuring, storage, use, disclosure by any means, and so on.

Sensitive personal data is a specific set of "special categories" that must be treated with extra security. Depending on the applicable law, this could include information pertaining to:

- Racial or ethnic origin;
- Political opinions;
- Membership of a political association;
- Religious or philosophical beliefs;
- Professional or trade union membership;
- Genetic data;
- Sexual orientation;
- Criminal records;
- Genetic information (that is not otherwise health information);
- Health information;
- Biometric templates;

- Biometric data (where processed to uniquely identify someone), etc.

The Company is the controller of the personal data collected within the Services, meaning we decide on why and how we collect certain data.

2. What Data Do We Collect?

1) Data we get from third parties

It is not necessary to create the account to access the App. In any case you will be given access to some basic App functionality. However, you can authorize in the App using your third-party account via Instagram. This will allow you to connect the App with your account on Instagram in order to repost content (posts (photos and/or videos), stories, reels, IGTV) (**'content'**) via Instagram.

When you authorize through Instagram, you may provide us access to all content of your Instagram account, and we will collect, store, and use the information you agreed such service could share with us from your social media account (e.g., your username, profile picture, content you intend to repost, mentioned location, post's description and other data of your social network account that will be transmitted for the purpose of authorization).

Keep in mind that these data are not necessarily required. Without such information, you will still be able to use our Services, but you won't be able to enjoy benefits that are available to registered users, for example, to repost content from a private Instagram account, as long as you don't provide us with access to your social media account.

If you decide not to authorize through Instagram, you also can repost content from other public Instagram accounts, accordingly, we will collect, store, and use the data of the other user whose content you reposted (e.g., username, profile picture, mentioned location, post's description and other available data of reposted content). As well as, the App will collect and store the list of content that you have reposted and content that you have copied and that is active to be reposted.

2) Data related to the use of the App

By adding text content to the photos you intend to repost, you can specify information in the text that will directly relate to you or other persons which, accordingly, will be personal data. We will not intentionally process this data, except to store and provide you with the Services within the functionality available in the App. We process only specific photos you chose to repost using the App. We do not collect your Instagram photos or photo albums.

3) Data related to your requests

When you send any request or message to the Company via Company's email address placed on the App, we may collect and process the data you voluntarily provide to us (e. g. your name, surname, email address, etc.). You can also specify other personal data in the request. We ask you not to provide us with excessive personal data, including the personal data of any third parties or sensitive data in your requests.

4) Newsletters

If you voluntarily provide to us your email, we will collect and further process your email address and your username to provide you our newsletters until you desire to opt out of such emails.

5) Financial information

Please pay attention that **we do not collect your payment credentials** (bank credentials, cards numbers and dates of issuance etc.). Such information may be collected exclusively by third-party payment providers with the respective licenses and security measures with regard to your payment credentials, as it is prescribed in our Terms. We receive only Transaction ID and Recipes from the third-party providers just to make sure that the transaction relates to you.

6) Automatically collected data

General information

We may automatically collect certain information about the devices you use to access the App. As described further below, we may collect and analyse (a) device information and identifiers such as IP addresses, location information (by country and city), unique device identifiers, Google Advertising ID, Apple ID for Advertising, IMEI and TCP/IP address, browser types, screen resolution, operating system, mobile device carrier information, mobile device language and (b) information related to the ways in which you interact with the App, such as platform type, the number of clicks, content viewed, statistical information about the use of the App (e.g. features you use; screens you viewed, navigation paths between pages or screens, the actions you take; the date and time you used the App, the frequency of your use of the App), error logs, and other similar information.

As described further below, we may use third-party mobile analytics services and technologies (such as Google Analytics, Firebase, AppStore Analytics, etc.), including cookies and similar tools, to assist in collecting this information. The information collected by various analytics technologies described in this section above will be disclosed to or collected directly by these service providers, who use the information to evaluate your use of the App, including by analyzing usage trends, assisting with fraud prevention, and providing certain features to you. Some of this information is collected using cookies and similar tracking technologies.

Cookies and similar technologies

Automated data collection helps us to automatically receive the information from your device and send the information back to improve your interaction with the Services and ensure its effective functioning.

Mobile devices may use other tracking files which are similar to cookies (for example iOS devices use Apple's Advertising Identifier and Identifier For Vendor). We use third-party software development kits SDKs, which are blocks of code provided by our analytics or advertising partners that we may install in our App. SDKs help these third parties and us understand how you interact with our Apps and collect certain information about the device and network you use to access the App. SDKs may collect the identifiers associated with your device or our Apps. Please refer to our partners' privacy and data sharing statements found on their respective websites for more information.

When you use the App, we may also use technologies like pixels, web beacons, and local storage to collect information about how you use App in order to:

- provide, improve, test, and monitor the effectiveness of the App;
- perform troubleshooting, diagnose or fix technology problems;
- enhance the safety and security of the App;
- monitor and analyse trends and usage;
- develop and test new functions of the App;
- understand your needs and provide services and advertisements that are relevant to you;
- use the information we've collected from cookies and similar technologies to enhance our App and your experience with it.

To express the choice not to have information about your use of mobile ads used for interest-based advertising purposes on your iOS mobile device, you should check the privacy settings on your device, changing the "Advertising"/ "Ads Personalization" settings.

If you opt-out of having your information collected and used by us and our third-party advertising partners for interest-based advertising purposes, you will still receive ads. The only thing we could do is to not tailor ads to your specific interests.

3. Lawful Basis and Purposes of Processing Your Data

Lawful basis

Performance of the contract. Our Services include the use of the App, their maintenance, as well as the user support and information services. We collect and process most of the personal data described in the Section above to fulfil our contractual obligations under our [Terms of Use](#), that is for the performance of the contract. Namely, the performance of the contract is the lawful basis for data related to your requests and when you authorise with a third-party account (Instagram). Besides, data related with use of the App also belongs to this category.

Your consent. If you wish to repost your or other users' content, we will ask you for your consent to add the copy of such content to the photo album on your device. We also collect and process your email you provide to us for the marketing purpose based on your consent in case you provide us with an email address through the App. We can send marketing and promotional emails to keep you informed of all changes, innovations, and improvements we make within the App. In no case we will overwhelm you with lots of letters. You can always choose to stop receiving our emails. If you want to cease this type of communication, simply use the "Unsubscribe" button which is present in each of our emails.

Legitimate interest. The legitimate interest is the legal basis for the processing when we process data to operate our App, ensure it works as intended and deliver the services you have requested. As well to analyse and aggregate data, to prepare statistics, in particular, to produce aggregated and anonymized analytics and reports, which we may use internally or share publicly or with third parties.

Our legitimate interest could also be in enhancing our App, adjusting App to the settings of your device, for example, automatically determining the language that is set on your device by default, testing and developing new features and carrying out analysis of our Apps so that we can optimise your user experience and provide you and other users with more efficient tools and features. Or we could have the legitimate interest to prevent or investigate possible wrongdoing in connection with the Services or to protect ourselves, our subcontractors, partners and affiliates against legal liability.

a. Purposes of processing

We collect and process the personal data described in the section above in order to provide you with all the necessary services within our Services.

In particular, we collect and process different types of data for the following purposes:

- **account data when a user authorises in the App using a third-party account** – in order to give you the ability to repost the content from the private users' Instagram accounts, identify the user and verify your identity;
- **data related to the use of App** – to ensure the App works as intended and deliver the services you want to receive under the Terms;

- **data related to your requests** – to communicate with you at your request, to provide a comprehensive answer to your inquiries, and to make sure that you are satisfied with our App, resolve your technical or other issues relating to the App;
- **data provided for receiving newsletters** – to send you our newsletters, keep you informed of all changes, innovations, and improvements we make within the Apps;
- **data collected through the automated collection** – depending on their type, we use them to make the usage of App possible. The purposes are different, depending on the variety of functions. For example, some are designed to adapt our App to the settings and specifications of your device, some of them are for analytical or statistical purposes, to test and develop new features, and carry out analysis of our App so that we can optimize your user experience and provide you and other users with more efficient tools and features. The others could help us to choose the best advertisements which would fit your interests, promote and drive engagement with the Apps. These activities we provide on the basis of our legitimate interests or your consent (where required). We do not use your data for these activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).

We may also use the data of any of the category above:

- to prevent, detect and report crime, protect you, other users and us, for example, by ensuring network and information security, mitigating security risks, detecting and preventing any fraudulent or malicious activity;
- to comply with any laws and regulations that apply to us;
- to exercise our rights set out in the Terms.

If we decide to change the purposes of processing specified above, we will inform you on such changes prior to the use of your personal data within the newly set purposes. Where applicable, you will have to provide your consent for the amended purposes (unless additional purpose of processing is compatible with those listed above).

4. How long do we store your data?

a. Retention period

Generally, we will not store any data you provide for longer than it is the specific Services required for the purposes described in this Privacy Policy. This means that our data retention periods will vary according to the reason for collection. After a retention period has elapsed, the personal data is securely deleted.

If you do not use the App for a certain amount of time, we will generally retain your personal data for you, such as your account information and reposted content, until you remain our user (this way, in the event that you delete your account on the App, we will immediately delete any personal data (with exception of some personal data relating to the provision of Services to you will be kept for a longer period, as long as necessary to comply with various finance- and tax-related legal obligations), provided under such account, including, but not limited to, your name, username, profile picture, logs, and any information on and from social networks, linked to such account).

Please note that except as required by applicable law or our specific agreements with you, we will not be obligated to retain your personal data for any particular period and we are free to securely delete it or restrict access to it for any reason and at any time, with or without notice to you. If you have any questions about our data retention policy, please contact us by e-mail at support@rpstservice.com. Please also note that we do not retain your payment information, as it is transferred directly to the relevant Service Provider

(such as Apple via in-app purchase mechanism). We only retain a token of such payment information (which cannot be used to re-identify you) and the chosen payment method.

Back-up period

We may, from time to time, back up all data placed within the Services. The data about your usage activity excluding personal data can be stored after your removal of the App, since we can periodically perform the back-ups of such data in order to reduce the risks of its destruction. This procedure allows us to maintain our Services and gives the possibility to restore the previous state of the Services in case of the breakage. That is, such backups may include, among other things, your personal data that we collected at the time the copy was made. To find out how to delete the information about your usage activity within the App, please visit the Apple Privacy Policy.

However, your data in the backups will only be used on the basis of our legitimate interest to restore our Services or your account if applicable under the Terms. We delete each back-up 1 month after it has been created.

a. Other processing

Please note that sometimes we may process your data for the period longer than indicated in this section. Such processing could be carried by us only for statistical purposes as it is provided for in Article 5 of the GDPR and subject to the appropriate safeguards in accordance with applicable data protection laws.

Statistical purposes mean any collection and processing of personal data necessary for statistical surveys or to produce statistical results. The statistical purpose implies that such statistical results do not include personal data, but only aggregate data. The statistical results may further be used for various purposes, for example, to assess our business development, understand the market demands and improve our Services.

In most cases, we will anonymize your data before starting processing it for statistical purposes. As a result, such data will no longer be considered personal and its use will be not governed by data protection laws.

5. Granting Access to Third Parties

To provide qualitative services, support various functions of our Services and ensure their operation, as well as to gather statistics and offer you personalised ads, we may hire people, work with service providers, partner companies, and organisations. For these reasons, they may access some of your personal data.

In all cases, we comply with the requirements of data protection legislation and make every effort to ensure that data processing is secure at all stages. Our subcontractors and any other third parties will provide the same or equal protection of your personal data as stated in this Privacy Policy.

Since some of your data may be transferred to third parties outside of the EEA, we could transfer such data on the basis of the standard contractual clauses signed with the respective third parties, if the country of transfer (like Ukraine or the USA) is not subject to the adequacy decisions of the European Commission. You may request the copy of such instruments via contact details provided in Section 11.

To achieve the purposes of data processing, we may provide your data to the following persons:

a. Our employees and independent contractors

We may pass on your data to our employees or verified independent contractors. We always enter into non-disclosure and confidentiality agreements with those employees and independent contractors who

have access to your data to ensure their data protection. We also sign the data processing agreements with them, where applicable.

b. Third-party services providers

The Company engages a number of trusted third-party service providers in order to support different features of our Services and ensure its overall functioning. We also use third-party services to organise our work in the most efficient way and provide our clients with the best customer service.

Therefore, we may grant such third-party service providers (and their subcontractors) [Google Analytics](#), [AppStore Analytics](#) and [Firebase](#) with a limited access to your personal data. We may also use other third-party services for analytics and marketing purposes. They help us to serve you with more useful and relevant ads and to measure their effectiveness. We never share your name or other information that directly identifies you when we do this. Instead, we use an advertising identifier like a device identifier.

As regards the engagement of the above-mentioned service providers, we take all necessary steps to ensure compliance with the applicable data protection laws such as the GDPR. In particular, we make sure that your personal data is being protected and used only within the purposes specified in this Privacy Policy. This is achieved by using only certified services and products, signing agreements on protection of personal data with contractors and partners, as well as taking technical measures to ensure the information is protected when stored, used and while being processed and transferred.

c. Other transfers required by law

We may also disclose your personal data to ensure compliance with the law. In other words, we may disclose information necessary for an investigation or trial at the official request of public authorities. If we are forced to disclose your information, we will notify you immediately and provide a copy of the request unless prohibited by law.

6. Your Data Processing Rights

To exercise your rights listed below, you can send a request to the Company to support@rpstservice.com. In order to properly protect your data, the Company may take additional measures to identify you when processing your request. We will provide you with a response to your request no later than 1 month from the date of its receipt, except as provided by law.

Thereby, you have the right to:

1. Know about the type of data processed, the sources of collection, the location of their personal data, the purpose of their processing, and the location of the owner or controller of personal data. The Policy was created to ensure this right. But you may ask us additional questions as to your data. You may receive information on the conditions for granting access to personal data, in particular information on third parties to whom your personal data is transferred. You may obtain a copy of your personal data.
2. Make a reasoned request to change or destroy their personal data if such data are processed illegally or are inaccurate, as well as in other cases provided by law. In particular, in the event of any inaccuracies in the data processed by the Company, the person whose personal data is processed has the right to contact us with a request to make appropriate changes to their personal data. You may also request that your data be destroyed if you believe that the Company no longer needs it for the purposes for which it was collected, you object or withdraw your consent.

However, we may retain certain personal data to the extent that processing is necessary to establish, assert or defend claims, as well as to fulfil a legal obligation requiring processing under EU law or the law of a Member State to which we are subject.

3. Withdraw consent to the processing of personal data. You can withdraw your consent to the processing of your personal data at any time in case the legal basis for the processing was the consent. In this case, we must stop processing, i.e., destroy or delete your personal data and notify you of the results.

However, there may be exceptions to this right. For example, if the law requires the Company to retain this data, or when it is necessary for the protection in litigation, or when the Company has other grounds for the processing, etc.

4. Object to data processing, if we process your data on the basis of legitimate interest. If you object and we do not have any other legal basis for the processing of personal data, we will delete your personal data, to the processing of which you have objected.
5. Make reservations about the restriction of the right to process your personal data while giving consent. If you submit such a request, pending its consideration, this may prevent you from the use of certain functionalities. Such requests could include questioning the correctness of your data, unlawfulness (if you do not want us to delete data), cases when we no longer need your data for the purposes collected.
6. Receive your personal data and send the data to another provider (data portability). We will send your personal data in the form of a csv file, which is a commonly used, machine-readable format that allows the received data to be sent to another personal data controller.
7. Complain about the processing of your personal data to the supervisory authorities or to the court and apply legal remedies in case of violating the data protection laws.
8. We do not make decisions about you based solely on automated processing (including profiling), which produces legal effects concerning you or similarly significantly affects you. You have the right to know the mechanism of automatic processing of personal data and the right to protection against an automated decision that has legal consequences for you. This provision is intended to protect the data subject from decisions made by the algorithm without human involvement or control. For example, if a computer program decides on the basis of certain collected information who needs help and who does not. To protect you against such a decision, if we implement one, we will explain the subject of the rules and logic of decision-making by the algorithm, as well as the ability to require a review of the decision by a person.

7. Privacy notice for California residents

This section supplements our Privacy Policy and is drafted to comply with our obligations under the California Consumer Privacy Act (CCPA).

It applies to you, if:

- your state of residence or establishment is California, or
- you are in California for any other purpose than a temporary or transitory purpose, or
- you are domiciled in California but are currently outside of the state for a temporary or transitory purpose.

a. Definitions

Please make sure you understand the important terms for California residents:

“Personal information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information could refer to:

- (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.
- (B) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an internet website, application, or advertisement.
- (C) Geolocation data.
- (D) Audio, electronic, visual, thermal, olfactory, or similar information.
- (E) Inferences drawn from any of the information identified in this list to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

“Processing” of the personal information means, for example, collection, recording, organizing, structuring, storage, use, disclosure whether or not by automated means etc.

“Sell” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.

b. Types of data we collect

Our App may collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device, including but not limited to identifying information (collectively, “personal information”). In particular, we collect the following categories of personal information from consumers:

- **Identifiers:** a real name, alias, unique personal identifier, online identifier, Internet Protocol address, email address, account name, or other similar identifiers.
- **Internet and other similar network activity:** information on a consumer's interaction with the App.
- **Sensory data:** visual information (especially images and video for stories, posts, reels, IGTV).

c. Disclosures of personal information for a business purpose

We disclose personal data for business purposes: primarily to perform analytics, but also to ensure the App works as intended, to fix errors, to protect the App from attacks etc. In the preceding twelve (12) months, we have disclosed for a business purpose personal information from category “Identifiers” and “Internet or other similar network activity”.

d. Sales of personal information

In the preceding (12) twelve months, pursuant to our App, we have sold personal information from category “Identifiers” and “Internet or other similar network activity”. To opt-out of the sale of your business email information, check the relevant section about it below.

Generally, we do not sell, trade or otherwise transfer to outside parties any personally identifiable information. This does not include trusted third parties or subcontractors who assist us in operating our App, conducting our business, or servicing you. Such trusted parties may have access to personally identifiable information on a need-to-know basis and will be contractually obliged to keep your information confidential. In particular, we use [Google Analytics](#), [AppStore Analytics](#) and [Firebase](#).

We may also release your information when we believe release is appropriate to comply with the law or protect our or others' rights, property, or safety. Furthermore, visitor information may be provided to other parties for marketing or other uses.

e. Your rights under the CCPA

Access (disclosure)

You may at any time obtain confirmation from us as to whether or not personal information concerning you are being processed. Namely, you have the right to request us to disclose to you the following:

- (1) The categories of personal information we have collected about you in the 12 months prior to the request.
- (2) The categories of sources from which the personal information is collected.
- (3) The business or commercial purpose for collecting or sharing personal information.
- (4) The categories of third parties with whom we share personal information.

Data portability

You may at any time order a complete data copy in a readily usable format, which you may further transmit to another controller. Logical relations between datasets will be preserved in the form of unique identifiers.

Right to opt-out

You can choose to opt-out of having your personal data "sold" or being used by third parties and businesses.

By informing us via email at support@rpstservice.com, you can restrict third-party providers to use your personal information. Third-party providers will only show you non-personalized ads. Non-personalized ads are based on contextual information, such as the content of our Services.

Cookie-based opt-outs are not effective on mobile applications. You may opt out of certain advertisements on mobile applications or reset advertising identifiers via their device settings. To learn how to limit ad tracking or to reset the advertising identifier on your iOS device, click on the following link:

[iOS](#)

You may also download and set your preferences on the App Choices mobile application(s) available in the App store.

Rights as to non-discrimination

We shall not discriminate against you because you exercised any of the consumer's rights under this Privacy Policy, including, but not limited to, by:

- (1) Denying the Services to you.
- (2) Charging different prices or rates for the services, including through the use of discounts or other benefits or imposing penalties.
- (3) Providing a different level or quality of the Services to you.
- (4) Suggesting that you will receive a different price or rate for the Services or a different level or quality of Services.

Deletion rights

You may without undue delay request the deletion of personal information concerning you, and we shall delete your personal information from our records, notify any service providers or contractors to delete

your personal information from their records, and notify all third parties with whom we have shared the personal information to delete your personal information.

We may refuse if this proves impossible or involves disproportionate effort. We shall not also be required to comply with your request if it is necessary for us to maintain your personal information in order to:

- (1) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
- (2) Debug to identify and repair errors that impair existing intended functionality.
- (3) Comply with the California Electronic Communications Privacy Act or the Penal Code, as well as with any other legal obligation.
- (4) Otherwise use your personal information, internally, in a lawful manner that is compatible with the context in which you provided the information.

We may maintain a confidential record of deletion requests solely for the purpose of preventing your personal information from being sold, for compliance with laws or for other purposes.

How to exercise rights

To exercise the access, data portability, and deletion rights described above, please submit a verifiable consumer request to us by emailing us at support@rpstservice.com. We will only use personal information provided in a verifiable consumer request to verify your identity or authority to make the request.

Only you, or an authorized person may make a verifiable consumer request related to your personal information. You may only make a verifiable consumer request for access or data portability twice within a 12-month period.

The verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority.

8. Your age

The privacy of children is one of our concerns. If you are a minor under the age of 18 (or the age of legal majority where you live) and at least 13 years of age, it is necessary that your parents or guardians look through this Policy and give their consent on your usage of the Services. It is especially important in case you would like to buy some of our paid Services. You are only permitted to use our Services through an account owned by a parent or legal guardian with their appropriate permission and under their direct supervision.

We do not intentionally collect any personal data concerning children under the age of 13 without verifiable parental consent. If we learn that we have inadvertently gathered personal data from a child under 13, we will take reasonable measures to promptly remove such data from our records.

9. Security of Personal Data

We take appropriate security measures to protect your personal data from accidental loss or destruction, from unlawful processing or access to it. For instance, all personnel are subject to full confidentiality and any subcontractors and subprocessors are required to sign a confidentiality agreement if not full confidentiality is part of the main agreement between the parties. Access to personal data is restricted to individually authorized personnel, we have implemented password hashing and two-factor authentication. We also implement other security measures which best fit the risks to your rights and freedoms.

Disclaimer. While taking necessary steps to secure your data, we have no choice but to admit that no method of transmission over the Internet or method of electronic storage is 100% secure. If it happens that any of your personal data is under the breach and if there is a high risk of violation of your rights as a data subject, we would inform you and the respective data protection authorities as to the accidents without undue delay. We will also do our best to minimize any such risks. Nonetheless, this disclaimer may not apply to you if the country of your residence provides that you are indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data.

10. Changes to this Privacy Policy

We may amend or update this Privacy Policy from time to time. If we decide to do so, and the amendments will substantially affect your rights and legitimate interests, we will notify you of any changes via email and/or a prominent notice within the App when you use the App for the first time after the amendments. We will also indicate the “Last modified” date at the top of this Privacy Policy.

11. Contact Information

If you have any questions about the Privacy Policy or your data being processed by **Elbax**, you are welcome to contact us:

Elbax OU

Narva mnt. 7-634, Harjumaa,
Tallinn, Estonia, 10117

General contact email: support@rpstservice.com