Privacy Notice

Last update 09.09.2021

Hacken OÜ understands how security is important. This Privacy Notice explains how and what data is stored, collected, and used while using our hPass by Hacken App.

In this Privacy Notice, we answer the following questions:

1. Who are we?

We are **Hacken OÜ**, located at Kai tn 1-5M, Tallinn city, Harju county, 10111, Estonia, registration code: 14351915. From now on, Hacken OÜ will be referred to as "we" and "our."

We are the controller of your personal data, which means that we determine what, for what purpose, and how we will process your personal data.

If you have any questions, you can contact us by sending an email to support@hacken.io. You can also send us a letter at the address: Kai tn 1-5M, Tallinn city, Harju county, 10111, Estonia.

2. What does this Privacy Notice cover?

This Privacy Notice applies to our hPass by Hacken App for iOS and Android.

3. What type of users do we have?

The data we process is divided into two categories: technical information and data provided to us by the **users** and **clients**.

Technical information. When you use our App, some data is collected automatically. We need technical data to operate, maintain, and improve our App. This includes data such as device type and OS version.

Data are provided to us by the following data subjects:

- **Users** — people who create an account in our App.
- **Clients** — people who already have an account at HackenAI.
- **HackenAI App** — our other product, an interactive tool to improve your personal security.

4. What data do we collect and why?

Please note: we do not have access to your personal data. All we have is an encrypted hash. To clarify, we do not know what you store. All your data, except email and device ID, is encrypted and stored on your device.

Mobile App hPass by Hacken does not have access to your biometric data, does not collect or store biometric data

How does it work?

We do not store data physically - it comes to us as encrypted, the seed phrase and master password or authentication via biometrics - in fact, it is a key to decrypt data when synchronizing the mobile application and account data on the server, stored in an encrypted form (we do not see and we do not know what is written there or saved)

But this data is stored via our App, so we explain to you what you can provide.

Data provided by the Users. We need only your email and device ID for verification (technical information) to provide the service.

You can store (so we are processing): master password, seed phrase (generated automatically), name, photo, passwords, notes, dates, logins, keys, seed phrases, secret notes, credit card details, verification. Again, we don't have access to this data.

Data provided by the Clients. To provide the service, we need email, device ID, and HackenID.

You can store (so we are processing): seed phrase (from HackenAI), name, photo, passwords, notes, dates, logins, keys, seed phrases, secret notes, credit card details, verification, technical information.

> Verification processing: we make a request to the operating system of the device, and it checks everything itself and gives us an answer whether that user or not.
>
> **Note:** you don't add a fingerprint or faceID- we only refer to your device (to operating system Apple (iOS) - Google (Android), which verifies the user's identity.
>
> You can use this function or not, and it's up to you.

HackenID. When you register an account in hPass, we screen our database to check if you have an account in HackenAI. We do this to:

- understand if you need to create a new account or just log in;
- synchronize data within your accounts.

Data provided by third parties. Information we can get from Google Analytics|Firebase, HackenAI: photo, name, email, comment, evaluation, password database.

Once again, briefly about what personal data we collect:

Type of data	Description of data	Legal basis	Reasons for processing
User			

You create an account	■ email; ■ master password; ■ seed phrase.	Performance of the contract	Registration, providing a service
You consent to the marketing	■ email.	Legitimate interest	Marketing
You contact us	■ email; ■ Name; ■ photo; ■ other information that may come to us through your email or other communication channels.	Legitimate interest	Marketing, support
You download passwords or add them	■ passwords; ■ login or email; ■ date; ■ notes.	Performance of the contract	Providing a service
You add a credit card	■ bank name; ■ card numbers; ■ cvv; ■ cardholder name; ■ exp. date.	Performance of the contract	Providing a service
You write a secret note	■ title; ■ note.	Performance of the contract	Providing a service
You add key	■ seed phrase; ■ note; ■ photo; ■ key (file).	Performance of the contract	Providing a service
Clients			

You create an account	■ email; ■ seed phrase (from Hacken AI); ■ HackenID.	Performance of the contract	Registration, providing a service
You consent to the marketing	■ email.	Legitimate interest	Marketing
You contact us	■ email; ■ Name; ■ photo; ■ other information that may come to us through your email or other communication channels.	Legitimate interest	Marketing, support
You download passwords or add them	■ passwords; ■ login or email; ■ date; ■ notes.	Performance of the contract	Providing a service
You add a credit card	■ bank name; ■ card numbers; ■ cvv; ■ card holder name; ■ exp. date.	Performance of the contract	Providing a service
You write a secret note	■ title; ■ note.	Performance of the contract	Providing a service
You add key	■ seed phrase; ■ note; ■ photo; ■ key (file).	Performance of the contract	Providing a service
Data provided by third parties			

You leave a review on the App Store or Google Play market	■ photo; ■ name; ■ email; ■ comment; ■ evaluation.	Legitimate interest	Analytics, support
You sign up with a HackenAI account	■ email; ■ password database.	Performance of the contract	improving the experience of using the application
Automatically collected data			
You use our App	technical information	Legitimate interest	App operation; Analytics; Statistics

Pay your attention. We knowingly **do not process** users' personal data under 18 without consent from a legal representative(s). If you are such a user or the user's legal representative, please let us know by email at support@hacken.io.

5. How long do we keep your data?

We store **users' and clients' data** for as long as the user uses our application and for three years afterward.

We store **technical data** for up to two years.

You can exercise your right to delete your data. In this case, we will delete your data from our servers within 30 days of your request.

The length of time we can retain **data from third parties** is determined by policies Google Analytics | Firebase, HackenAI.

6. Do we share data with third parties?

We use your personal data to perform a contract and for communication between the user and us. We use and transfer your personal data in measures that are needed to perform a contract. Also, we transfer your data on the following grounds:

Consent. We transfer your personal data based on your explicit consent.

Compliance with the law. We will disclose your personal data to third parties to the extent that it is necessary:

- to comply with a government request, court order, or applicable law;
- to prevent unlawful use of our App or violation of the Terms of Use of our App and our policies;
- to protect against claims of third parties;
- to help prevent or investigate fraud.

Transfer to third parties: We transfer your personal data to third parties based on a public offer for processing on our behalf, subject to technical and organizational measures to protect your personal data.

7. Do we do data transfer outside the European Economic Area?

The personal data we collect is stored on Google Cloud servers. The data is stored in Estonia by default, but we may need to process your personal data in another country.

8. What rights do I have regarding my data?

You, as subjects of personal data, have the following rights:

- **The right to access information.** You can request an explanation of the processing of your personal data.
- **The right to portability.** You can request all the data you provided to us and request to transfer data to another controller.
- **The right to restrict processing.** You may partially or wholly prohibit us from processing your personal data.
- **The right to file complaints.** If your request was not satisfied, you could file a complaint to the regulatory body.
- **The right to be forgotten.** You can send us a request to delete your personal data from our systems unless there is a legal requirement to keep it.

- **The right to withdraw consent.** You can always withdraw your consent to processing the data you have previously consented to, and we will stop processing it.

To exercise your rights, write us an email at support@hacken.io. We will answer you as soon as possible.

If your request was not satisfied, you can file a complaint to the Data Protection Inspectorate's regulatory body at info@aki.ee or write a letter to 39 Tatari St., 10134 Tallinn.

9. How do we update the Privacy Notice?

The GDPR regulates this Privacy Notice and the relationships falling under its effect. Existing laws and requirements for the processing of personal data are subject to change. In this case, we will publish a new version of the Privacy Notice in our app. If significant material changes are made that affect your privacy and confidentiality, we will notify you by email or display information on the App and ask for your consent.