



PRIVACY POLICY OF THE ACCOUNT INFORMATION SERVICE

This is the Privacy Policy for the Fincheck service provided by IDENTITY CONSORTIUM d.o.o., a company registered in the Republic of Croatia, with its address at Trogirska ulica 2, Varaždin, registration number: 070166678, Personal Identification Number (OIB): 44867795324 (hereinafter: "Identityum"). The service collects and analyses information on the User's account(s) and enables Users to provide the information thus collected to banks, payment institutions and other legal persons (hereinafter: "Third Parties") for the purpose of obtaining their financial products and/or services (hereinafter: the "Service").

Identityum has been entered by the Croatian National Bank in the Register of Payment Service Providers and Electronic Money Issuers pursuant to Article 130(1) of the Payment System Act (Official Gazette No 66/18) (hereinafter: the "Payment System Act"), under registration number AISP610 as of 29 June 2020. On this basis, Identityum is authorised, in accordance with the provisions of the Payment System Act, to provide the account information services described above.

1. GENERAL PROVISIONS

- 1.1. Identityum is the controller of the personal data provided by the User to Identityum for the purpose of and during the provision of the Services. As such, Identityum determines the purposes and means of processing the User's personal data.
- 1.2. This Privacy Policy aims to provide the User with information on how Identityum collects and processes all personal data collected from the User or provided by the User to Identityum.
- 1.3. Personal data means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2. METHODS OF DATA COLLECTION

- 2.1. Identityum collects personal data from the User through:
 - direct interactions, such as completing forms or communicating with Identityum in person, by email, telephone, post or otherwise. This includes personal data provided by the User to Identityum when registering to use the Service;
 - automated technologies or interactions with Identityum's website (www.identityum.com), through which Identityum may automatically collect technical data about the User's equipment, browsing actions and patterns. This personal data is collected, in particular, using cookies and other similar technologies, as described below in this Privacy Policy;
 - third parties or publicly available sources, for example, Google.

3. DATA COLLECTED AND PROCESSED

- 3.1. When providing the Service, Identityum collects and processes the following personal data of the User:
 - A. **personal and contact details** required to use the Services, including: first name and surname, address, age, email address and date of birth;



- B. **payment account and payment transaction information**, including payment account details (IBAN), payment account transaction details (transaction date, transaction amount, payer and payee, transaction description), categories of individual payment transactions and aggregate statistical indicators (aggregates, averages, minimums, maximums, etc.);
- C. **technical data** collected automatically when the User browses Identityum's Website, relating to the User's visit to the Website, including information about the device used by the User to access the Service (for example, mobile or web), the IP address used to connect the User's computer to the internet, the type and version of the User's browser, and the types and versions of browser plug-ins.
- 3.2. In particular, when providing the Service, Identityum will access, collect and process only the data referred to in Article 3.1 and will not access or collect sensitive payment data, namely data which can be used to carry out fraud, including personalised security credentials. Identityum shall ensure that personalised security credentials are not accessible to any person other than the User and the issuer of the credentials, and shall transmit them through safe and efficient channels within the communication session, in accordance with the Payment System Act (Official Gazette No 66/18).

4. LEGAL BASIS FOR THE COLLECTION AND PROCESSING OF PERSONAL DATA

- 4.1. Identityum will collect and process the User's personal data in the following circumstances:
- **to perform an Agreement** that Identityum is to enter into or has entered into with the User (i.e. when the User signs up for Identityum's Service and expressly accepts Identityum's General Terms and Conditions of the Service and this Privacy Policy, which together constitute the Agreement, thereby giving their consent to the provision of the Service);
 - **on the basis of consent** given by the User to Identityum (for example, for marketing);
 - **to protect Identityum's legitimate interests** (or those of a third party), where the User's interests and fundamental rights do not override those interests. Identityum will not collect or use the User's personal data for activities where the User's interests or fundamental rights and freedoms requiring the protection of personal data override those interests (unless the User has given prior consent to such processing or the processing is necessary for compliance with Identityum's legal obligations);
 - **to comply with a legal or regulatory obligation to which Identityum is subject.**
- 4.2. The following table describes all the ways in which Identityum processes and uses the User's personal data, the legal basis for processing the personal data and Identityum's legitimate interest, where applicable.

Purpose / Activity	Legal basis for processing personal data	Type of personal data
Entering into the Agreement for the provision of services	Performance of the Agreement	Identification and contact details
Performing and administering the Agreement entered into (e.g. sending notices)	Performance of the Agreement; contractual obligation	Email address
User participation in research/surveys	Consent	User statements / opinions / reviews
Publishing User statements / opinions / reviews on the Website	Consent	User statements / opinions / reviews



Purpose / Activity	Legal basis for processing personal data	Type of personal data
Providing the Services in accordance with the Agreement entered into	Performance of the Agreement	Account and financial information
Providing customer and technical support	Performance of the Agreement	Identification and contact details, account and financial information, technical data
Monitoring and improving the Service	Identityum's legitimate interests (to monitor use of the services and identify areas in which the Service or its functionality must or may be improved, including business and technical improvements)	Identification and contact details, technical data
Creating aggregated market research from which personal data will be removed	Identityum's legitimate interests (the market research is anonymised and, as such, sold to Identityum's clients to generate the revenue needed to provide the Services to Users free of charge)	Account and financial information, identification and contact details, all of which are anonymised
Using strictly necessary, functionality and analytical cookies	Identityum's legitimate interests (for the normal operation of the Website); consent	Technical data
Retaining business documentation in accordance with applicable laws and regulations	Compliance with a legal obligation	Financial documentation relating to the provision of the Service

4.3. Identityum may process the User's personal data on more than one lawful basis at the same time, depending on the specific purpose for which Identityum uses the personal data.

5. ACCESS TO DATA

5.1. Identityum may share the following categories of the User's personal data with the following third parties:

- the personal data referred to in Article 3.1, points A and B, of this Privacy Policy with third parties to whom the User has agreed that their personal data, payment account data and payment transaction data may be disclosed, as part of the provision of the Services and for the purpose of obtaining those third parties' financial products and/or financial or other services;
- the personal data referred to in Article 3.1, points A, B and C, of this Privacy Policy with legal persons providing services to Identityum to enable it to operate the Service and communicate with Users. These legal persons are authorised to use the personal data as processors and only to the extent necessary to provide Identityum's services. Their responsibilities for the protection of personal data are set out in a separate agreement concluded with Identityum;
- the personal data referred to in Article 3.1, points A, B and C, of this Privacy Policy with regulatory authorities or other public authorities that require reporting on personal data processing activities in certain circumstances. This includes, in particular, exchanging information with other legal persons and organisations for fraud protection and credit risk reduction purposes, and where disclosure is necessary to protect Identityum's rights, the safety of the User or others, or to investigate fraud;
- the personal data referred to in Article 3.1, point A, of this Privacy Policy with professional advisers, including lawyers, bankers, auditors and insurers providing consultancy,



banking, legal, insurance and accounting services, as processors and only to the extent necessary for Identityum to provide services to the User or fulfil its legal obligations. Their responsibilities for the protection of personal data are set out in a separate agreement concluded with Identityum;

- the personal data referred to in Article 3.1, points A, B and C, of this Privacy Policy with any third party on the basis of an agreement with the User. In such cases, Identityum will record that agreement in writing, specifying the purpose, frequency and duration of the data sharing, and will retain it in accordance with its data retention policy.
- 5.2. Where Identityum shares the User's personal data with third parties to whom the User has consented to the disclosure of their account and financial information as part of the provision of the Services and for the purpose of obtaining those third parties' financial products and/or financial services in accordance with Article 5.1, first indent, of this Privacy Policy, the agreed recipients, once the data has been disclosed to them, become separately and independently responsible for the further processing of and record-keeping relating to the User's personal data as independent controllers, in accordance with their own privacy policies.
- 5.3. If the User's personal data is transferred outside the EEA in accordance with this provision, Identityum will ensure that it receives the same level of protection by ensuring that at least one of the following safeguards is implemented:
- the country to which the data is transferred has been deemed by the European Commission to provide an adequate level of protection for personal data. For further details, see European Commission: Adequacy of the protection of personal data in non-EU countries;
 - where Identityum uses certain service providers based outside the EEA, it will use specific contracts approved by the European Commission which afford personal data the same protection as it has in EEA countries. For further details, see European Commission: Model contracts for the transfer of personal data to third countries;
 - where Identityum uses certain service providers based in the US, it may transfer data to them if they participate in the Privacy Shield, which requires them to provide protection for personal data similar to that applicable to personal data shared between Europe and the US. For further details, see European Commission: EU–US Privacy Shield.

6. USER RIGHTS

- 6.1. The User has the right to request a copy of the personal data held by Identityum about the User ("**right of access**"). This right enables the User to receive a copy of the personal data held by Identityum and to check that it is being processed on a lawful basis.
- 6.2. The User has the right to request the rectification of personal data processed by Identityum ("**right to rectification**"). This right enables the User to have incomplete or inaccurate data corrected.
- 6.3. The User has the right to ask Identityum to erase or remove personal data where there is no valid reason for Identityum to continue processing it ("**right to be forgotten**"). The User also has the right to ask Identityum to erase or remove their personal data where the User has successfully exercised their right to object to processing as set out in Article 6.4 of this Privacy Policy, where Identityum is processing the User's personal data unlawfully, or where erasure is required to comply with local law. However, Identityum may not always be able to comply with the User's request for erasure or removal of personal data for specific legal reasons, which will be notified to the User, where applicable, when the request for erasure or removal is made.



- 6.4. The User has the right to prevent Identityum from further processing the User's personal data for direct marketing purposes. Identityum will always inform the User if it intends to use the User's personal data for those purposes or disclose the User's data to a third party for those purposes. The User may also object to the processing of personal data based on Identityum's legitimate interests (or those of a third party), in particular where the User's specific situation leads them to conclude that the processing of personal data may affect their fundamental rights and freedoms ("**right to object and automated individual decision-making, including profiling**"). However, in that situation, Identityum may demonstrate that it has compelling legitimate grounds for processing the User's data which override the User's rights and fundamental freedoms.
- 6.5. The User has the right to ask Identityum to suspend further processing of personal data in the following circumstances ("**right to restriction of processing**"):
- where the User wishes Identityum to establish the accuracy of the data;
 - where the use of the data is unlawful but the User does not want Identityum to erase it;
 - where the User requires Identityum to continue holding their personal data, even if Identityum no longer has a need or interest in processing it, so that the User can establish, exercise or defend legal claims; or
 - where the User has objected to Identityum's use of personal data, but Identityum needs to verify whether it has overriding legitimate grounds to continue processing it.
- 6.6. In certain circumstances, the User may request the transfer of their personal data to the User or to a third party. Identityum will transfer the User's personal data to the User or a third party chosen by the User in a structured, commonly used and machine-readable format ("**right to data portability**"). However, this right applies only to automated data for which the User initially gave consent to processing or where processing was necessary to enter into a contract with the User.
- 6.7. Where the processing of personal data is based on the User's consent, the User may withdraw their consent at any time. Withdrawal of consent will not affect the lawfulness of processing carried out before consent was withdrawn ("**right to withdraw consent**").
- 6.8. Users may exercise any of the above rights by contacting Identityum at support@identityum.com.
- 6.9. Users do not have to pay a fee to access their personal data or to exercise any other right.
- 6.10. To ensure the User's right to access personal data or to exercise any other right, Identityum may request certain personal data from the User. This is a security measure to ensure that personal data is not disclosed to any person who is not entitled to receive it.
- 6.11. Identityum must respond to all justified requests from the User within 30 days. If a request is particularly complex or the User has made several requests, Identityum may take longer to respond, but no longer than 60 days from receipt of the request. In that case, Identityum will inform the User accordingly.

7. DATA RETENTION

- 7.1. Identityum will retain the User's personal data for as long as necessary to fulfil the purposes for which it was collected, including to satisfy any legal, accounting or reporting requirements.
- 7.2. When determining the appropriate retention period for personal data, Identityum will consider the amount, nature and sensitivity of the personal data, the potential risk of harm from its unauthorised use or disclosure, the purposes for which the data is processed, whether those purposes can be achieved by other means, and the applicable legal requirements.
- 7.3. Identityum normally retains personal data for up to 30 days after termination of the Agreement between the User and Identityum. After that period, Identityum deletes the personal data from



the system and it can no longer be accessed. In some circumstances, the User may ask Identityum to erase personal data earlier, as set out in Article 6.

- 7.4. Identityum also has certain legal obligations to retain records relating to the Services it has provided. Such records are retained for a maximum of 12 months after completion of the Service provided or for 5 years. If the Agreement is terminated, these records are archived and all other data is deleted.
- 7.5. Where Identityum anonymises personal data so that individual data can no longer be linked to a particular User and uses it for further research or statistical purposes, Identityum may use it indefinitely without further notice to the User.

8. SECURITY

- 8.1. With regard to the security of personal data, Identityum follows generally accepted industry standards to protect the personal data submitted to it, both during transmission and after receipt. However, no method of transmission over the internet or electronic storage is 100% secure. Therefore, Identityum cannot guarantee its absolute security.

9. LINKS TO OTHER WEBSITES

- 9.1. Identityum's Website may include links to third-party websites, plug-ins and applications. These include certain social networking features, such as the Facebook "Like" button or interactive mini-programs that run on the Website. Clicking on these links or enabling third-party features may allow the collection or sharing of the User's personal data. For example, these features may collect the User's IP address or the page the User is visiting and may set a cookie to enable the feature to function properly. These social media features and widgets are usually hosted by a third party or directly on the website. Identityum does not control these third-party websites or features and is not responsible for their privacy statements. The User's interactions with these features are governed by the privacy policy of the third party providing them.

10. COOKIES AND OTHER TRACKING TECHNOLOGIES

- 10.1. A cookie is a text file containing a small amount of information that is sent to the User's browser when the User visits a website. The cookie is then sent back to the originating website on each subsequent visit, or to another website that recognises it.
- 10.2. A web beacon is an often transparent graphic image, usually no larger than 1 pixel by 1 pixel, placed on a web page or in an email and used to monitor the behaviour of a User visiting a website or sending an email. It is often used in combination with cookies.
- 10.3. Identityum may collect data using cookies, web beacons or similar analytics-driven technologies.
- 10.4. Identityum uses the following cookies:
 - strictly necessary cookies, which are required for the operation of the website. These include, for example, cookies that enable the User to log in to secure areas of the website;
 - analytical/performance cookies, which enable Identityum to recognise and count the number of visitors to the website and to see how visitors move around it when using it. This helps Identityum improve the way the website works, for example, by ensuring that Users can easily find what they are looking for;
 - functionality cookies, which are used to recognise the User when they return to the website. This enables Identityum to personalise its content for individual Users, greet them by name and remember their preferences;



- targeting cookies, which record the User's visit to the website, the pages visited and the links followed. Identityum will use this information to make the website and the advertising displayed on it more relevant to the User's interests. Identityum may also share this information with third parties for this purpose.
- 10.5. Third parties (including, for example, advertising networks and providers of external services such as web traffic analysis services) may also use cookies over which Identityum has no control. These cookies are likely to be analytical/performance cookies or targeting cookies.
- 10.6. The User may block cookies by activating the setting in their browser that allows them to refuse all or some cookies. However, if browser settings are used to block all cookies, including strictly necessary cookies, the User may not be able to access all or parts of Identityum's website.

11. CHANGES TO THE PRIVACY POLICY

- 11.1. Identityum may unilaterally propose to the User amendments to the Agreement, namely to the provisions of this Privacy Policy, at least 2 (two) months before the intended effective date of such amendments.
- 11.2. Identityum shall send the proposed amendments referred to in the preceding paragraph of this Article to the email address designated by the User for this purpose. The amended text of the Privacy Policy shall be attached to that notice.
- 11.3. If, by the proposed effective date of the amendments to the Privacy Policy, the User has not notified Identityum in writing at support@identityum.com that they do not accept the proposed amendments, the User shall be deemed to have accepted them.
- 11.4. If the User does not accept the proposed amendments to the Agreement or the Privacy Policy and notifies Identityum in writing in accordance with Article 13.3 of this Privacy Policy, the User may terminate the Agreement with effect from any date before the effective date of those amendments, in accordance with Article 13 of the General Terms and Conditions. The General Terms and Conditions are available here (<https://identityum.com/terms-policies/>).

12. CHANGES TO PERSONAL DATA

- 12.1. It is important that the User's personal data processed and held by Identityum is accurate and up to date. Users should therefore notify Identityum promptly if their personal data changes during the term of the Agreement between Identityum and the User.