General Terms and Conditions for the Use of the Rekono Service

Version:	4.7
Date of issue:	January 23, 2025
Date of entry into force:	January 27, 2025

Document protection

Document custodian:	Adviser to the CEO of Rekono d.o.o.
Document approver:	CEO of Rekono d.o.o.
Scope of validity:	Rekono work areas related to the provision of the Rekono e-identification and the services for remote e-signature, e-seal and time-stamp within Rekono Sign

Document version control

The original document is stored electronically and the versions of the document are under control. Paper or electronic copies of the document may exist for distribution to those to whom the document is addressed or who need to consult it in the course of their work. Copies of the document are not controlled and should be treated as such by the reader.

Change history of the document:

Date	View version at	Description / Note
01.05.2016	1.0	Version 1.0
11.09.2019	2.0	Adaptation of policies for customers of the banks
01.04.2020	3.0	Rekono.TSP and Rekono OnePass added
16.11.2020	4.0	Identification procedures, authentication mechanisms and registration authority added
16.12.2020	4.1	Minor corrections and additions
19.12.2020	4.2	Minor corrections and additions
09.01.2021	4.3	Minor corrections and additions
26.01.2021	4.4	Minor corrections and additions
16.09.2022	4.5	Minor corrections and additions
14.12.2022	4.6	Minor corrections and additions to terminology
09.01.2025	4.7	Change to corporate identity and minor additions

Table of contents

1. GENERAL

1. These General Terms and Conditions govern the use of the Rekono online electronic identification and authentication service (hereinafter referred to as the "Rekono Service") provided to users by Rekono d.o.o. (hereinafter referred to as "Rekono" or the "Controller"). By accepting the General Terms and Conditions and registering their legal identity by opening an Account in the Rekono System (hereinafter referred to as the "Rekono Account"), the User acquires the right to use their Rekono Account with the selected authentication elements and authentication procedure in trust services for electronic transactions and in other solutions or services of providers of online and other electronic services that require reliable and secure representation and confirmation (authentication) of the User's identity in order to access these services.

2. By registering and opening a Rekono Account, the User enters into a contractual relationship with Rekono for the use of the Rekono Services in accordance with these General Terms and Conditions and the accompanying instructions. The concluded contract is also the legal basis for the processing of the User's personal data within the Rekono System and the Rekono Services, with the exception of the location data of the User of the Rekono OnePass service, for the processing of which the Controller has a demonstrated legitimate interest.

3. When the User opens a Rekono Account in connection with the commencement of the use of a service of a particular service provider (e.g. a bank, an insurance company or other financial organization, a telecommunications operator, etc.), the User may also be obliged to comply with additional terms and conditions of the service provider when using the Rekono Account.

4. The Rekono TSP Policy and the Rekono Service operating descriptions in the versions valid at the time of the adoption of the General Terms and Conditions are an integral part of the General Terms and Conditions and can be viewed at www.rekono.si.

5. The Rekono TSP Policy, which can be viewed at https://www.rekono.si/pravila-rekono-tsp/, also forms an integral part of these General Terms and Conditions.

2. TERMS AND ABBREVIATIONS

2.1. Terms used in these General Terms and Conditions have the following meanings:

a) "Biometric data" means data about a person's physical characteristics, such as a fingerprint, an image of a face or cornea, captured by a mobile device using embedded sensors and processed for the purpose of authorizing the person to use the mobile device or its SIM card. This data is only stored on the person's mobile device and is not accessible to Rekono, but can be used as one of the elements to authenticate the person.

b) An "authentication element" is a factor that is demonstrably linked to an individual and falls into (at least) one of the following categories:
   - A "possession-based authentication element" (something that is in the sole possession of the User) is an authentication factor for which a person must prove that they are in possession;
   - A "knowledge-based authentication element" (something that only the User knows) is an authentication factor for which a person must prove that they have knowledge of it;
   - An "inherent authentication element" (something the User is) is an authentication factor based on a physical characteristic of a natural person for which the person must prove that they possess that physical characteristic.

c) "Rekono OnePass" is a mobile application for implementing strong two-factor User authentication using push notifications and one-time passwords (TOTP).

d) "SMS-OTP" is a one-time password for logging into your Rekono account, sent to your cell phone via SMS.

e) "User" is a natural person who uses a Rekono Account as an individual or as a representative of a legal entity.

f) "Credible Source" means any source that in any way reliably provides accurate data, information and/or evidence that can be used to prove a person's identity.

g) "Strong authentication" means authentication using two or more elements that fall into the categories of knowledge (something that only the User knows), ownership (something that only the User owns), and inherent connection to the User (something that the User is), that are independent of each other, meaning that a breach of one element does not compromise the trustworthiness of the others, and that are designed to protect the confidentiality of the information being authenticated.

h) "Secure Online Shopping" means online shopping at retail stores that use the Mastercard SecureCode, Mastercard Identity Check and Visa Secure online payment service.
i) "Rekono 3D Secure" means a service that enables cardholders to make secure online purchases using Mastercard Identity Check and Visa Secure (also known as 3D Secure 2.0).
j) "Rekono TSP" means a qualified Trust Service Provider for:
    - the issuance of certificates for electronic signatures, certificates for electronic seals and certificates for the provision of other trust services;
    - the validation of electronic signatures or electronic seals; and
    - the creation of electronic time stamps.

Other terms used in these General Terms and Conditions have the same meaning as in Regulation (EU) No 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/EC (hereinafter referred to as the "eIDAS Regulation"), in the implementing regulations issued on the basis of the eIDAS Regulation and in the Act on Electronic Identification and Trust Services (Official Journal of the Republic of Slovenia, No. 121/21 and 189/21 - ZDU-1M and REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 11, 2024 amending Regulation (EU) No 910/2014 as regards the establishment of a European digital identity framework).

2.2. Abbreviations and other terms

PAN	Primary Account Number (PAN)
PIN	Personal Identification Number (PIN)
TSP	Trust Service Provider (TSP)
SMS-OTP	One-time passwords sent to the cell phone
FIDO	Open Standard for Authentication, https://fidoalliance.org/ (Fast IDentity Online)
passkey	A more secure alternative to passwords, login by fingerprint, facial recognition, etc.
chip	electronic element, integrated miniature circuit

3. REGISTERING AND USING THE REKONO ACCOUNT

1. The User obtains the right to use the Rekono Account by registering on the website www.rekono.si and accepting the Terms and Conditions by clicking on the "I accept the Terms and Conditions" checkbox, which activates the Rekono Account.

2. The level of trust in the User's identity, as demonstrated and guaranteed by the Rekono Account, depends on the Rekono Account registration and activation procedure, the procedure for verifying and validating the User's identity, the authentication elements used and the way the Rekono Account is managed. The procedures listed above are implemented in Rekono in accordance with the requirements of Regulation (EU) No. 910/2014 and the Commission Implementing Regulation (EU) 2015/1502 issued on the basis thereof, as well as the relevant technical specifications and standards.

3. The Rekono Service consists of the issuance and management of Rekono Accounts of the following levels of assurance:

a) very low (0), which provides low trust in the User's claimed and stated identity and slightly reduces the risk of misuse or alteration of the User's identity;
b) low (10), which provides limited trust in the User's claimed and stated identity and is intended to reduce the risk of the misuse or alteration of the User's identity. This level corresponds to the eIDAS low assurance level;
c) medium (20), which provides medium trust in the User's claimed and stated identity and aims to significantly reduce the risk of misuse or alteration of the User's identity. This level corresponds to the eIDAS medium assurance level;
d) high (30), which provides a higher level of trust in the User's claimed and stated identity and aims to prevent the risk of misuse or alteration of the User's identity. This level of assurance corresponds to the eIDAS high assurance level.

4. The following authentication elements are available to the User within the Rekono Account:

a) username and password - the username is the email address provided by the User when registering for a Rekono Account, while the password is a

string of characters that the User must provide when registering for a Rekono Account;

b) push notifications sent and confirmed in the Rekono OnePass application, which is part of the Rekono Service;
c) TOTP Authenticator for mobile devices - generates time-varying one-time passwords (TOTP). Only the Rekono OnePASS application, which is part of the Rekono Service, can be used;
d) FIDO devices - physical authentication with a compatible FIDO device;
e) passkey technology - physical authentication with a compatible implementation of passkey technology;
f) SMS-OTP - one-time passwords sent to your cell phone via SMS;
g) qualified certificate - registration and use of qualified certificates from certification service providers registered in Slovenia;
h) a high-level electronic means of identification issued in the form of a digital certificate stored on the chip of an ID card.

5. When registering an authentication element, Rekono always performs a proof-of-possession of ownership for the authentication elements to be used by a specific user. The verification is performed for all the elements listed in the previous paragraph, namely:

a) to confirm the possession of an email address, Rekono sends an email with a confirmation code to the User's email address;
b) to validate the Rekono OnePass mobile application, the User must log in with a Rekono Account and go through a strong authentication process;
c) to confirm possession of a cell phone for SMS OTP, Rekono will send a one-time password to confirm ownership to the cell phone number, provided by the User during registration;
d) to confirm possession of a qualified certificate, the User must log in with their valid qualified certificate;
e) to confirm ownership of a FIDO device or the implementation of passkey technology, the User must prove ownership by activating the device.
f) a high-level electronic means of identification in the form of a digital certificate stored on the chip of an ID card.

6. The authentication elements available in the Rekono Account provide the User with strong two-factor authentication. To demonstrate and ensure a medium or high level of trust in their identity, the User must in their Rekono Account:

a) register their valid qualified certificate, or

b) verify their identity with the registration authority of the trust service provider that issued the qualified certificate to the User; or
c) complete the registration with a valid PAN and PIN combination of their card, or
d) complete identity confirmation with the Rekono registration authority.
e) register a high-level electronic means of identification issued in the form of a digital certificate stored on the chip of an identity card.

The Rekono Account authentication elements may only be used to authenticate a User in the Rekono System.

7. For a very low level of trust in the User's Rekono Account, it is sufficient to confirm possession of the electronic means of identification (email address and telephone number) and to agree to the General Terms and Conditions.

8. For a low level of trust in a User's Rekono Account, it is sufficient to confirm the identity verification by checking external registers based on the information provided by the User.

9. For a medium level of trust in a User's Rekono Account, it is sufficient for the User to register:

a) with an existing qualified certificate, or
b) with a valid PAN and PIN combination of their payment card issued after the bank has established and verified their identity remotely, without the need to be present in person, in accordance with the provisions of the Prevention of Money Laundering and Terrorist Financing Act; or
c) by having their identity confirmed by an external provider for whom the Conformity Assessment Body has certified the reliability of a procedure equivalent to physical presence, or
d) by confirming their identity through remote identification by the Rekono registration authority.

Confirmation of identity by means of a) and c) fulfills the conditions for issuing a qualified certificate.

10. In order to have a high level of trust in the User's Rekono Account, the User must:

a) confirm their identity with the Rekono registration authority, which will establish and verify their identity by inspecting their official photo ID in

their personal presence and by checking their identification data in the Central Register of Residents and the Tax Register, or

b) register a valid qualified certificate, issued on a qualified electronic signature creation device, in their Rekono Account, or
c) register with a valid combination of the cell phone number previously entered in the cardholder's banking system, the PAN number and the PIN of their payment card issued by the bank after their identity has been established and verified by inspecting their official photo ID in their personal presence, in accordance with the Act on the Prevention of Money Laundering and Terrorist Financing; or
d) register in their Rekono Account a valid high-level electronic means of identification in the form of a digital certificate stored on a chip of the ID card.

The confirmation of identity by means of (a), (b), (c) and (d) fulfills the conditions for the issuance of a qualified certificate.

11. A User authenticated with a Rekono Account that provides a low, medium or high level of trust in their identity can use Rekono Sign to remotely create:

a) an advanced electronic signature;
b) an advanced electronic signature with a qualified certificate;
c) a qualified electronic signature
d) an advanced or a qualified electronic seal;
e) an advanced or qualified electronic time stamp;
f) the verification of the validity of an electronic signature or seal; and
g) in connection with the creation of an electronic signature, the issuance of an advanced and qualified electronic time stamp.

4. SECURE ONLINE SHOPPING WITH REKONO 3D SECURE

1. Rekono 3D Secure ("Rekono 3D Secure") is a service for the secure validation of online purchases in online retail stores, available to the cardholder via the Rekono OnePass mobile application or the alternative solution Rekono SMS OTP. To use either of these solutions, the cardholder must register a Rekono Account, which is set to a medium or high assurance level after the payment card details have been entered and verified.

2. Rekono 3D Secure is available to Rekono Account Users who are payment cardholders of banks with which Rekono has entered into an agreement to provide this service (hereinafter referred to as the "Bank"). The use of Rekono 3D Secure is free of charge for all Users.

3. In addition to these General Terms and Conditions, when using Rekono 3D Secure, the User is obliged to comply with the terms and conditions set by the Bank for online purchases with Mastercard ID Check and Visa Secure.

4. The payment cardholder can register a Rekono Account via the Rekono OnePass mobile application or on the rekono.si website, where a description of the registration process is also available.

5. The User activates the secure online purchase confirmation service in the Rekono OnePass mobile application or online via the Rekono Account Control Panel, by entering the number of one of their payment cards (PAN) and the corresponding personal identification number (PIN). The PIN data is not stored in the Rekono OnePass application, but is encrypted with the processing center's (i.e. Bankart) encryption key, and sent to the issuing bank of the payment card used, and stored there.

6. The activation of one payment card activates all of the User's payment cards at the issuing bank of the activated card.

7. When using the Rekono OnePass mobile application for secure online purchase, the User will receive a push notification to review the purchase details and confirm the purchase. Making a secure online purchase can be prevented if there are factors that pose a high risk of misuse.

8. For users who do not have a smartphone or do not wish to use the Rekono OnePass mobile application for payment confirmation, there is alternatively the Rekono SMS OTP solution, where the User enters the password previously set up in the Rekono Account for online purchases into the browser during the confirmation process at the online point of sale, as well as a secure one-time password sent by SMS to the cell phone number with which the User has registered their Rekono Account.

9. For online purchases with Mastercard Identity Check and Visa Secure, the cardholder does not present their card number, but authenticates their identity within the Rekono OnePass application when they receive a push notification for a secure online purchase, or with their password for secure online purchases and with a one-time secure password that they receive by SMS message.

10. When using the Rekono SMS OTP solution, for each purchase at an online point of sale that supports the use of Mastercard and Visa Secure Identity Check, the User must enter their Secure Online Purchase password that they set up in their Rekono Account when activating the Secure Online Purchase service, as well as the one-time secure password that they receive in the SMS message before making the purchase.

11. When using the Rekono OnePass mobile application, each time the User makes a purchase at an online point of sale that supports the use of the Mastercard Identity Check and Visa Secure service, the User must confirm the execution of the payment using push notification received before the purchase via the Rekono OnePass mobile application.

12. When making a secure online purchase, the User is only required to enter a secure one-time password or confirm the push notification if the screen requesting the password entry or confirmation displays the correct merchant, the correct amount and the correct last four (4) digits of the User's payment card, which the User must verify. The absence or inaccuracy of the above information on the screen may indicate that a website is attempting to obtain the cardholder's identification data with the intention of misusing it. In this case, the Cardholder must not enter the secure one-time password or confirm the push notification and must close the web browser or the Rekono OnePass application immediately.

13. The security and confidentiality of the mobile device on which the User receives secure one-time passwords or on which the Rekono OnePass mobile application is installed is the sole responsibility of the User, who is obliged to keep it safe in order to prevent its loss, theft and/or misuse (e.g. by locking the screen with a password, PIN or a sample of their fingerprint).

14. The User is obliged to immediately notify the Bank that issued the payment card and/or Rekono of the loss, theft and/or misuse of the mobile device as well as of any unauthorized use of the secure one-time passwords or suspicion that their Rekono Account or other data and devices used to perform the secure online purchase confirmation service on their behalf have been or may be misused by another person. The User should be aware that they are responsible for all payments for secure online purchases confirmed with Rekono OnePass or Rekono SMS OTP based on a login with their Rekono Account, regardless of whether they have been a victim of fraud.

15. Rekono shall not be liable to the User for any damages of any kind resulting from the use or attempted use of Rekono 3D Secure by the User or from the deactivation, modification or interruption of the operation of Rekono 3D Secure.

16. Rekono may suspend or terminate the provision of this service at any time at the request of a Bank that uses Rekono 3D Secure to issue payment confirmation for secure online purchases to its cardholders.

17. The Controllers of the personal data of Users who validate payments for secure online purchases with Rekona 3D Secure are the Banks, each for their own payment cardholders. Rekono has a entered into an agreement with each of the Banks for the processing of Rekono 3D Secure Users' data in accordance with the General Data Protection Regulation.

5. DATA PROCESSING AND PROTECTION OF USER RIGHTS

1. Rekono keeps a register of Rekono Accounts users, which contains the following information:

a) the User's personal name,
b) specifying the procedure for establishing and confirming the User's identity when registering a Rekono Account or an e-identification means,
c) the type and number of the User's valid official identification document used with a photograph,
d) the User's tax identification number or Unique Master Citizen Number or other user identifier (e.g. PIN) if required for registration and determining the trust level of the Rekono Account or e-identification means,
e) a unique electronic identification number (UIN),
f) the User's permanent or temporary residence, if required for registration and setting the trust level of the Rekono Account or the e-identification means,
g) the User's cell phone number, if required for registration and setting the trust level of the Rekono Account or e-identification means,
h) the User's email address, if required for registration and use of the Rekono Account,
i) the location of the Rekono OnePass user;
j) the status of your Rekono Account,
k) the period of validity of your Rekono Account,
l) the period of suspension of the Rekono Account,
m) the date of termination of the Rekono Account.

2. The Rekono System processes different sets of personal data about the User depending on the level of trustworthiness of the Rekono Account:

a) Level "0": the User's email address and the number of the cell phone to which they receive SMS messages;
b) level '10': level '0' data + name and surname, date of birth, tax number, EŠEI and address of residence, number and validity of the official identification document;
c) Level "20" and "30": level "10" data + qualified certificate.

The purpose of the processing of data relating to the User of a Rekono Account and the authentication elements used as part of this Account is to provide the User with

electronic identification and authentication services at a level that enables the User to use the Rekono Trust Services and the electronic services of the providers relying on those services.

4. The purpose of the processing of Rekono OnePass User location data is to prevent misuse. The data is stored as an additional attribute in the log records and is used by the system to detect and prevent abuse.

(5) The Controller may, at the request of the User, provide the User's data from the Rekono Account to the extent necessary for the performance of a particular identification/authentication procedure or trust service to the electronic service provider relying on that procedure or service.

6. The data of each Rekono Account shall be kept for 10 years after the end of the validity of the account.

7. Automated decision-making or profiling is not carried out in the context of the Rekono Services.

8. in relation to the processing of the data of the User's Rekono Account, the User has the right to request from the Controller access to and rectification or erasure of personal data or restriction of processing in relation to the User, the right to object to processing and the right to data portability. The request of the data subject shall be treated in accordance with the provisions of the General Regulation. The address for exercising the rights in relation to data processing is info@rekono.si.

9. On the Information Commissioner's website, Users can submit a complaint for breaches of legislation on the protection of personal data using the form.

6. RESPONSIBLE USE AND TERMINATION OR REVOCATION OF THE USE OF A REKONO ACCOUNT

1. To prevent misuse of the Rekono Account, the User must use the authentication elements or procedures with due care and responsibility. It is the responsibility of the User to select the most appropriate authentication element for the purpose and manner of use of the Rekono Account.

2. The User must update any changes to their registration details in the Rekono Account without delay.

3. To prevent misuse of the Rekono Account, the User must handle the data of the authentication elements used to access the Rekono Account with care, so that they are not disclosed to others and to prevent any possible misuse of this data or the Rekono Account.

4. The User must immediately report any suspected misuse of their data or authentication elements for accessing their Rekono Account to the Controller by email to info@rekono.si.

5. The User is liable for all damages caused by the User's provision or negligent use of their data to access and use the Rekono Account.

6. The User may terminate the use of the Rekono Account at any time by using the "Terminate User Account" function in the Rekono Account Control Panel. Upon termination, the User's data in the Rekono Account will be stored and deleted in accordance with the regulations on electronic identification and trust services and the protection of personal data.

7. The Controller may block access to a particular Rekono Account after repeated unsuccessful attempts to log in with the selected authentication element.

8. In the event of misuse of the Rekono Account, the Controller may revoke the User's right to use the Account with immediate effect and store the User's data in accordance with the regulations governing electronic identification and trust services and the protection of personal data.

9. The Controller shall not be liable for any damages or other consequences arising from the misuse of the Rekono Account by the User or a third party or from the revocation of the right to use the Rekono Account. This applies in particular to the following:

a) if the User gives their authentication elements or Rekono Account to another individual for use by the latter to falsely represent the User's identity in legal transactions,
b) if the User, using the identity authenticated through the Rekono Account, harasses, threatens or harms other persons through unsolicited advertising or otherwise,
c) if the User, using the identity provided and claimed with the Rekono Account, violates legal restrictions (e.g. copyright laws, prohibitions, personality rights under criminal and civil law) when retrieving and storing, transmitting, distributing or displaying certain content,
d) if the User fails to stop or prevent the perceived misuse of their data for the use of the Rekono Account,
e) if the User, alone or in cooperation with another, uses the authentication with their Rekono Account for unauthorized analysis of system functions of the Rekono Services or data in devices, databases or services or for manipulation of such data and/or documents,
f) any misuse resulting from or having the appearance of a criminal offense by a third party.

10. The Rekono Account will be automatically terminated in the event of inactive use of the account for a period of 3 years.

7. PROTECTION OF THE CONFIDENTIALITY OF REKONO ACCOUNT DATA, MEANS AND METHODS OF IDENTIFICATION AND PROVISION OF AUDIT TRAILS

1. The Controller shall protect the User Data and other data related to the User's Rekono Account in accordance with the requirements of the General Data Protection Regulation, the applicable personal data protection law and the Controller's internal act on ensuring the security of the processing of personal data. The Controller holds ISO 9001, ISO/IEC 27001 and ISO/IEC 20000-1 certificates.

2. The User shall protect the confidentiality of the Rekono Account data, in particular the authentication elements and procedures, and shall use them in accordance with these General Terms and Conditions and the instructions for the use of the Rekono Account or the individual authentication elements, if any. In the event of negligent conduct or misuse of the Rekono Account that has harmful consequences for Rekono or other users of the Rekono Services, the User may be liable for damages or criminal prosecution.

3. The User is obliged to take special care to protect the identification code that indicates ownership of the Rekono Account (the so-called PUK code), which allows the User to access and reset their Rekono Account if they have forgotten their password or lost ownership of other means of e-identification.

4. Every use of the Rekono Account by the User and every access to the Rekono Account data by other authorized persons ("Audit Trails") shall be recorded in a dedicated Rekono data repository, with each audit trail record being signed with a private key stored on a secure hardware device. The stored audit trails shall only be used by the Controller for the purpose of dealing with the User's requests for the protection of their rights in relation to the processing of data concerning them and for statistical processing for the purpose of improving the services or the functioning of the Rekono System. The Controller may, on the basis of lawful requests, transmit the Audit Trail record to the competent state authorities.

8. THE COST OF USING A REKONO ACCOUNT

1. The registration and use of a Rekono Account of trust level "0" and "10" is free of charge for the User.

2. The costs of registering and using a Rekono Account of trust levels '20' and '30' are normally linked to the use of a trust service of a specific provider, which shall determine how they are charged.

9. RIGHTS AND OBLIGATIONS OF THE CONTROLLER

1. In the event of misuse of the Rekono Service, the Controller may block the User's use of the Rekono Account with immediate effect and shall immediately take other necessary precautions and procedures to limit the consequences of the misuse.

2. The Controller undertakes to maintain the availability of the Rekono Service for the User until the termination of the use of the Rekono Service and to store and delete the User's data in the Rekono Account after the termination of the User relationship in accordance with the relevant regulations.

10. AVAILABILITY OF THE REKONO SERVICES

1. The Rekono Services are available to the User 24 hours a day, seven days a week. Due to the occasional need to carry out service and maintenance work on the systems, Rekono may be temporarily unavailable during this period. The Controller expressly points out that temporary inability to use the services can never be completely excluded. In this respect, the Controller shall only be liable for damages resulting from the unavailability of the Rekono Services caused by its gross negligence or willful misconduct. Liability for consequential damages or loss of profit is excluded in its entirety.

2. The Controller shall not be liable if the User can only access the Rekono Account on a limited basis or not at all, if this is due to technical components (e.g. hardware and software) or the availability of Internet access at the User's premises.

11. COOKIES

1. The rekono.si website uses cookies to ensure the smooth operation of the service. You consent to the use of cookies by using our services. For more information on cookies, please read the "**Website Visitor Privacy Policy**" and the "**Cookie Policy**", available at https://www.rekono.si/splosni-pogoji/.

12. CHANGES TO THE REKONO SERVICES AND GENERAL TERMS AND CONDITIONS

1. The Controller may amend or supplement the General Terms and Conditions from time to time as required by changes in the content or the way in which the Rekono Services operate:

a) new or amended regulations;
b) regulators or changes to technical specifications or standards; or
c) identified needs to improve Services or functioning of the Rekono System.

2. If the update affects the use of the Services or the legal rights of a Rekono Account User, the Controller shall notify Users at least 15 days before the date on which the update takes effect by sending emails to the email addresses associated with the Rekono Accounts and by posting a notice on the www.rekono.si website. If an individual User does not agree with the notified updates, they may cancel their Rekono Account before the changes become effective. By using the Services or accessing the Rekono Account after the updates have come into effect, the User signifies their acceptance of the new General Terms and Conditions and the amended contractual relationship with the Controller relating to the use of the Rekono Account.

13. DISPUTE RESOLUTION

1. The User may send any questions, complaints or requests regarding the use of the Rekono Account and the Rekono Services, as well as regarding the security of their personal data when using the Rekono Service, to info@rekono.si. The Controller will endeavor to reply as soon as possible, and at the latest within the time limits set by law.

2. The Controller shall endeavor to resolve any disputes arising out of this Agreement amicably, but if this is not possible, such disputes shall be settled by a competent court in Ljubljana.

14. REFERENCES

(1) REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation)

(2) COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of September 8, 2015 laying down minimum technical specifications and procedures for trust levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No .../.... 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eID IUK)

(3) Electronic Commerce and Electronic Signatures Act - ZEPEP (Official Journal of the Republic of Slovenia, No 98/04 - official consolidated version, No 61/06 - ZEPT and No 46/14)

(4) Prevention of Money Laundering and Terrorist Financing Act - ZPPDFT-2 (Official Gazette of the Republic of Slovenia, No. 47/2022)

(5) Payment Services, Electronic Money Issuing Services and Payment Systems Act - ZPlaSSIED (Official Journal of the Republic of Slovenia, No. 7/18, 9/18 - corrected version and 102/20)

(6) Electronic Identification and Trust Services Act - ZEISZ (Official Journal of the RS, No. 121/21 and 189/21 - ZDU-1M)

(7) COMMISSION DELEGATED REGULATION (EU) 2018/389 of November 27, 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards for communication (RTS SCA)

(8) Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(9) REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 11, 2024 amending Regulation (EU) No 910/2014 as regards the establishment of a European Digital Identity Framework

(10) COMMISSION DELEGATED REGULATION (EU) 2022/2360 of August 3, 2022 amending the regulatory technical standards laid down in Delegated Regulation (EU) 2018/389 as regards the 90-day account access exemption