# General Terms and Conditions for the Use of the Rekono Service

Ljubljana, December 15, 2022

**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 Rekono e-identification and remote e-signature, e-seal and time stamp services within Rekono.Sign**

## 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 proven legitimate interest.

3. When the User opens a Rekono Account in connection with the commencement of the use of a service of a specific 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 descriptions of the functioning of the Rekono Service in the versions valid at the time of acceptance of the General Terms and Conditions are an integral part of the General Terms and Conditions and are available at www.rekono.si.

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

# 2. TERMS AND ABBREVIATIONS

## 2.1. The 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:
- "possession-based authentication element" (something that is solely in the possession of the User) is an authentication factor that requires an individual to prove that it is their possession;
- "knowledge-based authentication element" (something known only to the User) is an authentication factor for which an individual must prove that they have knowledge of it;
- "inherent authentication element" (something that is the User) is an authentication factor that is based on a physical characteristic of a natural person and 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 a Rekono Account, that is sent to the User's cell phone via SMS.

e) »User« means a natural person who uses the Rekono Account as an individual or as a representative of a legal entity.

f) »Credible source« means a source in any form that 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 affect 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« refers to a service that enables payment cardholders to make secure online purchases using Mastercard Identity Check and Visa Secure (also known as 3D Secure 2.0).

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 adopted on the basis of the eIDAS Regulation, and in the Electronic Identification and Trust Services Act (Official Journal of the Republic of Slovenia, No. 121/21 and 189/21 - ZDU-1M).

## 2.2. Abbreviations

| | |
|---|---|
| PAN | Payment Card Number |
| PIN | Personal Identification Number |
| TSP | Trust Service Provider |
| SMS-OTP | One-time passwords sent to the cell phone |
| FIDO | Open standard for authentication, https://fidoalliance.org/ (Fast IDentity Online) |

## 3. REGISTRATION AND USE OF 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 General Terms and Conditions« checkbox, thus activating 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 confirming the User's identity, the authentication elements used and the way in which 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 adopted on the basis thereof, as well as the relevant technical specifications and standards.

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

a) very low (0), which provides low trust in the User's 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 identity, and is intended to reduce the risk of 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 provided identity, and aims to significantly reduce the risk of misuse or alteration of the User's identity. This assurance level corresponds to the eIDAS medium assurance level;
d) High (30), which provides a higher level of trust in the User's identity being proven and provided 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 the Rekono Account, and the password is a string of characters that must be provided by the User when registering the Rekono Account;
b) push notifications sent and confirmed in the Rekono OnePass application, which is part of the Rekono Service;

c) TOTP Authenticator mobile app - 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) SMS OTP – one-time passwords sent via SMS to a cell phone;
f) qualified certificate - registration and use of qualified certificates from certification service providers registered in Slovenia.
g) 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 elements listed in the previous paragraph, namely:

a) to confirm the possession of an e-mail address, Rekono sends an e-mail with a confirmation code to the User at that 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 the 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 possession of a FIDO device, 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 a valid qualified certificate; or
b) validate their identity with the registration authority of the trust service provider issuing 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) a high-level electronic means of identification issued in the form of a digital certificate stored on the chip of an ID card.

The authentication elements of the Rekono Account may only be used to authenticate the 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 (e-mail address and telephone number) and agree to the general terms and conditions.

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

9. For a medium level of trust in the 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 his/her payment card issued after the bank has established and verified his/her identity remotely and without his/her personal presence, in accordance with the provisions of the Act on the Prevention of Money Laundering and Terrorist Financing; or
c) by confirming his/her identity through an external provider certified by the Conformity Assessment Body as reliable by a procedure equivalent to physical presence; or
d) by confirming their identity through remote identification with the Rekono registration office.

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 prove his/her identity:

a) confirm his/her identity with the Rekono registration authority, which will establish and verify his/her identity by inspecting his/her official photo ID in his/her personal presence and by checking his/her 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 his or her 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 number of his/her payment card issued by the bank, after his/her identity has been established and verified by inspecting the official photo ID in his personal presence, or

d) register in his/her Rekono Account a valid high-level electronic means of identification in the form of a digital certificate stored on the chip of an identity card.

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

11. Rekono Account authentication, which provides a medium or high level of trust in the User's identity, allows the User to remotely sign, using the Rekono.Sign Service:

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

# 4. SAFE ONLINE SHOPPING WITH REKONO 3D SECURE

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

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 using the Mastercard ID Check and Visa Secure services.

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

5. The User activates the service for secure confirmation of online purchases within 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 OnPass application, but is encrypted with the processing center’s encryption key, (i.e. Bankart’s encryption key), and sent to and stored by the issuing bank of the payment card used.

6. Activating 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, the User will receive a push notification to check the purchase details and confirm the purchase in order to confirm the payment for a secure online purchase. Making a secure online purchase can be prevented if there are factors that pose a high risk of abuse.

8. For Users who do not have a smartphone or do not wish to use the Rekono OnePass mobile application for payment confirmation, an alternative Rekono SMS OTP solution is available, where the User enters in the browser the password for online purchases that they have previously set up for their Rekono Account during the confirmation of a purchase at an online point of sale, as well as secure one-time password that they receive by SMS to the cell phone number under which they have 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 in the Rekono OnePass application when they receive a push notification for a secure online purchase, or with their password for secure online purchases and a one-time secure password that they receive by SMS.

10. In the case of 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, which they set up in their Rekono Account when activating the Secure Online Purchase service, and the secure one-time password they receive in the SMS message before the purchase.

11. In the case of 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 the push notification received before the purchase via the Rekono OnePass mobile application.

12. When making a secure online purchase, the User will only 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 is required to 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 details with the intention of misusing them. 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 his/her fingerprint).

14. The User is obliged to immediately inform 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 the unauthorized use of the secure one-time passwords or of the 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 damage resulting from the User's use or attempted use of Rekono 3D Secure or from the deactivation, modification or interruption of Rekono 3D Secure.

16. Rekono may suspend or discontinue 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 Rekono 3D Secure are the banks, each for their own payment cardholders. Rekono has 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 manages the User record of the Rekono Account, which contains the following data:

   a) the User's personal name,
   b) the details of the procedure for establishing and confirming the User's identity when registering for a Rekono Account or e-identification means,
   c) the type and number of the User's valid official photo ID used,
   d) the User tax number or Slovenia Unique Master Citizen Number (EMŠO) or other User identifier (e.g. PIN), if required for registration and setting the security level of the Rekono Account or e-identification means,
   e) a unique electronic identification number (UIN),
   f) the permanent or temporary residence of the User, if this is required for registration and setting the trust level of the Rekono Account or e-identification means,
   g) the User's cell phone number, if required for registration and setting the trust level of the Rekono Account or the e-identification means,
   h) the User's e-mail address, if required for registration and use of the Rekono Account,
   i) the location of the Rekono OnePass User;
   j) the status of the Rekono Account,
   k) the period of validity of the 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 the User's personal data depending on the trustworthiness of the Rekono Account:
   a) level »0«: the User's e-mail address and the number of their cell phone to which they receive SMS messages;
   b) level »10«: level »0« data + first and last name, date of birth, tax number, UIN and residential address, number and validity of official ID;
   c) level »20« and »30«: level »10« data + qualified certificate.

3. The purpose of processing the data of 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 Rekono trust services and the electronic services

of providers that rely on these services.

4. The purpose of processing the location data of the User of the Rekono OnePass Service 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 misuse.

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

6. The data of each Rekono Account will be retained for a period of ten years after the expiry of the Account.

7. Automated decision-making or profiling does not take place in the context of Rekono Services.

8. With regard to the processing of the User's Rekono Account data, the User has the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the personal data, as well as the right to object to processing and the right to data portability. The data subject’s request will be handled in accordance with the provisions of the General Regulation. The address for exercising rights in relation to data processing is info@rekono.si.

9. On the Information Commissioner’s website, the User can submit a complaint about violations of personal data protection legislation using a form.

# 6. RESPONSIBLE USE AND TERMINATION OR WITHDRAWAL OF USE OF THE REKONO ACCOUNT

1. In order to prevent misuse of the Rekono Account, the User must use the authentication elements or procedures with due care and responsibility. The user is responsible for selecting the most appropriate authentication element for the purpose and type of use of the Rekono Account.

2. The User must immediately update any changes to its registration data in the Rekono Account.

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

4. The User must immediately report any suspicion of misuse of their data or the authentication elements used to access their Rekono Account to the Controller by sending an e-mail to info@rekono.si.

5. The User is liable for all damages caused by the 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 Clicking »Terminate User Account« in the Rekono Account control panel. After 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 personal data protection.

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

8. in the event of misuse of a 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 on electronic identification and trust services and the protection of personal data.

9. The Controller shall not be liable for any damage or other consequences resulting from the misuse of the Rekono Account by 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 provides his/her authentication elements or the Rekono Account to another person for use in order to misrepresent the identity of the User in legal transactions,
b) if the User uses the identity authenticated via the Rekono Account to harass, threaten or harm other persons through unsolicited advertising or in any other form,
c) if the User violates legal restrictions (e.g. copyright laws, prohibitions, personal rights under criminal and civil law) with the identity provided and claimed via the Rekono Account when retrieving and storing, transmitting, distributing or displaying certain content),
d) if the User fails to prevent or stop the identifiable misuse of its data for the use of the Rekono Account,
e) if the User alone or in collaboration with another uses the authentication with its Rekono Account to analyze or manipulate system functions of the Rekono Services or data in devices, databases or services without authorization, or to manipulate such data and/or documents,
f) any misuse resulting from a criminal offense 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 protects the User's data and other data related to the User's Rekono Account in accordance with the requirements of the General Data Protection Regulation, the applicable law on the protection of personal data and the Controller's internal act on ensuring security in the processing of personal data. The Controller holds the ISO 9001, ISO/IEC 27001 and ISO/IEC 20000-1 certificates.

2. The User is obliged to maintain the confidentiality of the Rekono Account data, in particular the authentication elements and procedures, and to use them in accordance with these General Terms and Conditions and the instructions for using the Rekono Account or the individual authentication elements, if any. In the event of negligent behavior 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 prosecuted.

3. The User is obliged to protect with particular care the identification code that indicates the ownership of the Rekono Account (the so-called PUK code) and that allows the User to access and reset his/her Rekono Account if he/she has forgotten his/her password or lost possession 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 (i.e. audit trails) is recorded in a dedicated Rekono data repository, with each audit trail record signed with a private key stored on a secure hardware device. The stored audit trails are used by the controller only to process requests from the User for the protection of his/her rights in connection with the processing of the data concerning him/her 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 records of the audit trail to the competent state authorities.

# 8. COSTS FOR THE USE OF THE 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 for the registration and use a Rekono Account of trust level »20« and »30« are generally linked to the use of the trust service of the specific provider, who determines how they are calculated.

# 9. RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

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

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

# 10. AVAILABILITY OF THE REKONO SERVICES

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

2. The Controller is not liable if the User can only access the Rekono Account to a limited extent 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. Rekono.si uses cookies to ensure the proper functioning of the service. By using our services, you agree to the use of cookies. For more information about cookies, please read the Privacy Policy of the website rekono.si[1].

[1] https://www.rekono.si/sl/politika-zasebnosti/

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

1. The Controller may amend or supplement the General Terms and Conditions from time to time if this is necessary due to changes in the content or operation of the Rekono Services:

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

2. If an update affects the use of the Services or the legal rights of a Rekono Account User, the Controller will notify Users at least 15 days before the update takes effect by sending emails to the email addresses associated with the Rekono Accounts and 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 take effect. By using the Services or accessing the Rekono Account after the updates take effect, the User agrees to the new General Terms and Conditions and the amended contractual relationship with the Controller in relation to the use of the Rekono Account.

## 13. DISPUTE RESOLUTION

1. The User may address 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 data Controller will endeavor to respond as soon as possible, but at the latest within the legal deadlines.

2. The Controller shall endeavor to settle any disputes arising from this Agreement amicably, but if this is not possible, the disputes shall be settled by the 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 means of electronic identification 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 (IUK eID)

(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 Journal of the Republic of Slovenia, No. 47/2022)

(5) Payment Services, Services of Issuing Electronic Money 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 Republic of Slovenia, No. 121/21 and 189/21 – ZDU-1M)

(7) COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 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 of communication (RTS SCA)

(8) Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons 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)