XRPL Labs
PRIVACY NOTICE

Your privacy matters to us. In this Privacy Notice we explain how The Integrators B.V., acting under the trade name XRPL Labs (**XRPL Labs** or **we**) uses your personal data we collect through our mobile application (**XUMM App**) and the third-party in-app apps, such as the XUMM Support, Tangem Backup, Account Worth, (**xApps**) (together, the **mobile application**), and our interactions with you via the mobile application.

XRPL Labs is a Dutch registered and located company and we process your personal data under / in accordance with the General Data Protection Regulation (**GDPR**).

We may change this Privacy Notice from time to time. At all times, we will publish the up-to-date version in our mobile application, together with a summary of key changes. If we make any important changes to this Privacy Notice (e.g. regarding the personal data we collect, how we use it or why we use it), we will notify you.

This Privacy Notice explains the following:

1 WHO IS THE DATA CONTROLLER?

The controller for our mobile application is The Integrators B.V., acting under the trade name 'XRPL-Labs', Schothorsterlaan 11, 3822 NA Amersfoort, The Netherlands.

If you have any questions or complaints in relation to the use of your personal data or if you would like to receive more information about how XRPL Labs processes your personal data, please contact us through the communication mechanism in the XUMM app (XUMM Support xApp), via e-mail: compliance@xumm.app, or by sending a registered letter to XRPL Labs, Schothorsterlaan 11, 3822NA Amersfoort, The Netherlands.

2 HOW DO WE COLLECT YOUR PERSONAL DATA?

Your personal data is (i) provided by you; and/or (ii) obtained from third parties (e.g. Veriff in relation to the AML and sanction checks, XRP Forensics for transaction monitoring, and Zendesk for support information).

3 THE TYPES OF PERSONAL DATA WE COLLECT FOR OUR PURPOSES AND THE APPLICABLE LEGAL BASIS FOR OUR DATA PROCESSING?

In the context of your use of the mobile application, we collect, store and use personal data about you as set out in the "personal data" column below. You will also find below the purpose of the processing and the legal basis we rely on for each type of personal data that we process about you.

Depending on your use of the mobile application, we process different types of personal data from you. You can either be a:

- **Mobile application user** (not using any further services of XRPL Labs and/or having an account to use the XRPL Labs services)
- **XRPL Labs client/customer** (having an account to use the XRRL Labs services, XUMM Pro subscription).

Based on the above, we created two tables:

Mobile application user		
Personal data	**Purpose**	**Legal basis**
Data related to the use of the mobile application, such as: • XRP ledger wallet address • Country connecting from Preferences regarding services and products.	Facilitating the mobile application, including maintaining and ensuring a secured online environment on our mobile application and the services offered through them.	Necessary for the purpose of our legitimate interests to provide the mobile application to you, and to maintain and improve the mobile application. Necessary for the purpose of our legitimate interest, namely, to maintain a secure online environment on our application

XRPL Labs client/customer		
Personal data	**Purpose**	**Legal basis**
Data related to the use of the mobile application, such as: • XRP ledger wallet address • Country connecting from Preferences regarding services and products.	Facilitating the mobile application, including maintaining and ensuring a secured online environment on our mobile application and the services offered through them.	Necessary for the purpose of our legitimate interests to provide the mobile application to you, and to maintain and improve the mobile application. Necessary for the purpose of our legitimate interest, namely, to maintain a secure online environment on our application
Account data*, such as: • Full name • Address • Email address • Date of birth • Telephone number • IP address • User content (such as profile photo, comments and other materials (if uploaded by user)) • KYC data (see below). * *(onboarding XUMM Pro subscription, on-ramp/off-ramp onboarding)*	Keep and maintain an accurate and adequate profile administration. For general use of the mobile application, including, if applicable, onboarding identification and verification. User content: customizing your mobile application experience to your preferences, including sending push notifications, personalizing your profile with a profile picture of you and your comments / chats in the mobile application.	Necessary for the purpose of our contractual relationship with you. Necessary for the purpose of our legitimate interests to maintain an adequate profile administration. Necessary for compliance with a legal obligation to carry out an identification and verification process (e.g. the Money Laundering and Terrorism Financing Prevention Act). Processing user content is based on your consent.
Order data, such as: • Full name • Delivery address • Email address • Telephone number • Banking details (exchange only) • Order history.	Manage and process the order. For example, ordering a Tangem card, or any other physical product from us.	Necessary for the purpose of our contractual relationship with you to manage your order provided through the mobile application.

XRPL Labs client/customer		
Personal data	**Purpose**	**Legal basis**
Regulated currency exchange data, such as: • Bank account number • Bank account name • Transaction amount • Transaction history • XRP ledger wallet address.	For providing regulated currency exchange services.	Necessary for the purpose of our contractual relationship with you.
Customer experience data, such as: • Experience • Source of income • Why exchange functionality • Source owned XRP.	For the Xumm Pro subscription onboarding identification and verification, and the use of third parties for verification and data completing purposes. For legal obligations to process customer and transaction data and to provide personal data to supervisory authorities (AML and sanction law obligations).	Necessary for the purpose of our contractual relationship with you. Necessary for compliance with a legal obligation which are applicable to XRPL Labs for AML and sanction law obligations.
Communication data, such as: • Full name • Email • Communication history.	Facilitate the provision of a communication tool.	Necessary for the purpose of our legitimate interests to facilitate the provision of a communication tool.
Promotion data (direct marketing communication), such as: • Full name • Email • Country.	Sending direct marketing communications.	Consent.
Know Your Customer (KYC) data, such as: • Copy ID document • Copy utility bill	For carrying out our standard due diligence process for identification and verification.	Necessary for the purpose of our contractual relationship with you. Necessary for compliance with a legal obligation to carry out an identification

XRPL Labs client/customer		
Personal data	**Purpose**	**Legal basis**
• Bank statement • Credit card statement • Photo / video and metadata of the image (mobile phone type, operating system, provider) • GPS information about the image's location.		and verification process (e.g. the Money Laundering and Terrorism Financing Prevention Act).

4 WITH WHOM WE SHARE THE PERSONAL DATA?

To the extent applicable, we will disclose or share your personal data with the following third parties:

Party	Purpose
AFAS	For our primary service offering and our backoffice processes, we use services and tools from AFAS. This (ERP) system will hold all personal data from customers.
Cloudflare	For data traffic from the application to our platform. Malware and DDOS management/monitoring.
DigitalOcean	Hosting provider for infrastructure, support and order form services.
Firebase (by Google)	For push notification delivery and crash report collection with the mobile application. (Google already has the data. If you decide to use this, the data can be connected to the mobile application users.)
Hetzner	Hosting provider for infrastructure, support and order form services. Fallback cluster if Digital Ocean would be unavailable.
Stripe	Online payments for creditcard payments for the Tangem cards.

Veriff SDK	For the KYC procedure, AML and sanction checks.
External courier providers (for national and international shipments), including, but not limited to, DHL.	For the sending and customs checks of products, such as the Tangem Card.
Zendesk	Support software related to customer support.

Further, we may disclose or share your personal data:

- to our group entities for business purposes, including administrative, management and accounting purposes, and as part of our regular reporting activities on company performance, in the context of a business reorganization or group restructuring exercise, for system maintenance support and hosting of data;
- if we sell our company or part thereof (including separate assets), or if we merge with another company. In such event, we may share your personal data with the new owner or merging party respectively, but only to the extent necessary for the purpose for which your personal data are processed;
- if we are subject to insolvency proceedings, as part of the sale of our assets by a liquidator (or similar); or
- we are legally obliged or allowed to do so. In such event we shall share your personal data with the relevant supervisory authority, investigative authority or other governmental body.

5 HOW LONG DO WE RETAIN YOUR PERSONAL DATA?

We do not process your personal data any longer than necessary for the processing purpose.

In this context, we keep your personal data for as long as your account is active or as necessary to provide our services to you.

More information

Mobile application user	
	Retention Period
Data related to the use of the mobile application	6 weeks (log files are deleted every 6 weeks).

XRPL Labs client/customer	
	Retention Period

Data related to the use of the mobile application	6 weeks (log files are deleted every 6 weeks).
Account data	• General: five years after the last exchange / transaction, or five years after our contractual relationship has ended (e.g. termination of the subscription (customer relationship with XRPL Labs)). • User content: for as long the user profile photo, comments and other materials (if uploaded by user) • KYC data: see retention period below.
Order data	Two weeks after delivery.
Regulated currency exchange data	Five years after the customer initiated the exchange transaction.
Customer experience data	Five years after we were required to report the exchange transaction.
Communication data	• 30 days after the last contact with you. ○ If the communication data includes support data, this data is being anonymized after 30 days and retained for development, legal and business purposes.
Promotion data	Until you opt-out of receiving promotional emails or messages.
KYC data	Five years after completed KYC (verification / identification) procedure.

If we are subject to a statutory retention period, we will retain your personal data for the period specified by the law. For example, financial administration needs to be retained for a period of 7 years after the relevant fiscal year.

Notwithstanding the above, we may retain your personal data for the length of any applicable limitation period for claims that might be brought against us later.

In some circumstances, we may anonymize your personal data so that it can no longer be associated with you, in which case we may use such data without further notice to you.

6 HOW DO WE APPLY AUTOMATED DECISION-MAKING AND PROFILING

The GDPR defines automated decision-making (including profiling) as the ability to make decisions by technological means without significant human involvement. Profiling involves the automated processing of personal data with a view to evaluating or predicting personal aspects such as the economic situation, reliability or likely behaviour of a person. In automated decision-making without profiling, personal aspects are not taken into account for evaluation or prediction.

In providing you with our support we use our support platform Zendesk, which uses ticket information to auto-replay to your questions. This is based on machine learning, certain questions usually resolve with certain answers. Automated decisions without the use of profiling are permitted by the GDPR Implementation Act.

In order to identify money laundering and, as such, fulfil regulatory requirements, we use customer contact data, transaction data from the historic exchanges with our mobile application and transaction data from the XRP ledger linked to the customer XRP Ledger wallet for the profiling of the customer (creating a customer profile). This profiling is required by law, and based on these

profiles we can decide to not (or no longer) provide our services. We do not automatically decide on the basis of profiling as defined in the GDPR. However, we make use of personal aspects (contact data and transaction data) for identifying money laundering and fulfilling of regulatory requirements. Profiles created in this way are always assessed by a human being and that person also makes the decision.

7 WHERE DO WE STORE YOUR PERSONAL DATA?

Mobile application user
XRPL Labs stores your personal data on servers located within the European Union, namely in the Netherlands.

XRPL Labs client/customer
XRPL Labs stores your personal data on servers located within the European Union, namely in the Netherlands. Our main processes and services are located and stored within the European Union. Some of our processors and other parties with whom we share your personal data may store your personal data in other locations. If we share your personal data in accordance with this Privacy Notice with third parties, we take steps to ensure that we meet any applicable requirements under the applicable privacy and data protection laws.

8 HOW WE SECURE YOUR PERSONAL DATA

We maintain appropriate organisational and technological safeguards to help protect against unauthorised use, access to or accidental loss, alteration or destruction of personal data.

See below more information regarding our safeguards

Data limitation	We limit the data that we collect. Only data we need to provide the services are collected and only stored for the time we need to process the data to provide the services, taking into account regulatory requirements on retention periods.
	Data that is not directly needed to provide the services in the mobile application, but are needed to fulfil contractual or legal requirements, are stored offline, meaning the data is not available on public networks and is not available on our private network. The data is held on a server or backup facility not connected to our network.
Data encryption	The data is encrypted, with solid key management tooling and techniques. The keys are managed by one person, with two additional people being able to access the keys if the first person is not available. However, all processes are implemented and automated not to have to access the keys.
Access limitation	Access to servers, databases and platforms is granted on a least privilege basis, and only accessible by employees using private key encryption,

	only from whitelisted IP addresses (e.g. work & home). For remote work a VPN connection is required. All machines & infrastructure are firewalled.
Data minimisation	When processing personal data is no longer necessary, but the data is needed for analytical purposes, the data is anonymised. For example, the support tickets, where after the ticket has been dealt with, we remove the personal data but keep the classified issue for historical purposes and trend analysis.
Integrity and confidentiality	All of our employees use password vaults to store their passwords. The vault is only accessible through multi factor authentication.
Security audits	We provide the source code of the XUMM App as open-source so that the security of the XUMM app can be checked and challenged by the general public. Also, we subject the XUMM App (the app source code) to periodical & ongoing security audits (Cossack Labs).

9 WHAT ARE YOUR RIGHTS?

You have the right to access your personal data, the right to have your personal data rectified or erased, the right to restriction of the processing, the right to data portability and the right to object to the processing. Most of these rights are not absolute and are subject to exemptions in the law.

Below we set out your rights in more detail and give information on how you can exercise these.

We will respond to your exercise of right request within one month, but have the right to extend this period to two months. If we extend the response period, we will let you know within one month from your request.

- **Access:** you are entitled to ask us if we are processing your personal data and, if we are, you can request access to your personal data. This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it. If your request is clearly unfounded or excessive we reserve the right to charge a reasonable fee or refuse to comply in such circumstances.

- **Correction or updating:** you are entitled to request that any incomplete or inaccurate personal data we hold about you is corrected.

- **Erasure (deletion):** you are entitled to ask us to delete or remove personal data in certain circumstances. There are certain exceptions where we may refuse a request for erasure, for example, where the personal data is required for compliance with law or in connection with legal claims. When we need to rely on an exemption, we will inform you about this.

- **Restriction:** you are entitled to ask us to suspend the processing of certain of your personal data about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Data portability:** you may request the transfer of a copy of certain of your personal data to you or another party (if technically feasible). You have the right to ask that we provide your personal data in an easily readable format to another company. Please note, this right applies

to the personal data you have provided to us and only if we use your personal data on the basis of consent or where we used your personal data to perform a contract with you.

- **Objection:** where we are processing your personal data based on our legitimate interest, you may object to processing on this ground. You also have a right to object where we are processing your personal data for the purposes of direct marketing or profiling. You can object at any time and we shall stop processing the information you have objected to, unless we can show compelling legitimate grounds to continue that processing.

- **Withdraw your consent.** Where you have provided your consent to our processing of your personal data you can withdraw your consent at any time. If you do withdraw consent, it will not affect the lawfulness of what we have done with your personal data before you withdrew consent.

If you exercise the rights above and there is any question about who you are, we may require you to provide information from which we can satisfy ourselves as to your identity.

If you want to exercise any of these rights, or withdraw your consent, please send us an email via support@xumm.app.

10 HOW CAN YOU LODGE A COMPLAINT WITH A SUPERVISORY AUTHORITY?

If you have any complaint about the way we process your personal data, you may lodge a complaint with a supervisory authority in the country of your residence, where you work or where an alleged infringement of the applicable data protection law took place. A list of EU supervisory authorities and their contact details is available here.