IntmaxWallet privacy policy

Version 1.0 – March 2023

About us

This privacy policy ("**Privacy Policy**") explains how we process and protect your personal data when you (the "**user**" or "**you**") use our website https://intmax.io/ or our services provided via https://intmaxwallet-app-web.vercel.app/ (together, the "**Services**").

The Services are operated by Ryodan Systems AG, Hirschengraben 40, 6003 Luzern, Switzerland (the "**Company**", "**we**", "**our**", or "**us"**). The Company is the controller for the data processing described below.

Unless otherwise defined in this Privacy Policy or our General Terms & Conditions, the definitions used in this Privacy Policy have the same meaning as in the Swiss Federal Act on Data Protection or the EU General Data Protection Regulation.

1 Personal data we collect

We may collect or receive personal information for a number of purposes connected with our business operations when you use our Services. This may include the following:

- Login details
- Wallet address

2 How we collect personal data

We collect information about our users when they use Services, including taking certain actions within it.

Directly

- When users access, use, or otherwise interact with our Services.

Indirectly

- Through public sources.

3 Legal basis and purposes

Our legal basis for collecting and using the personal data described in this Privacy Policy depends on the personal data we collect and the specific purposes for which we collect it.

Contract: To perform our contractual obligations or take steps linked to a contract with you. In particular:

- To provide our services.

Consent: We may rely on your freely given consent at the time you provided your personal data. In particular:

- To provide you with news, special offers, newsletters, and general information about goods and services which we offer.

Legitimate interests: We may rely on legitimate interests based on our assessment that the processing is fair and reasonable and does not override your interests or fundamental rights and freedoms. In particular:

- To maintain and improve our Services.
- To develop new services.
- To defend against legal claims and in legal proceedings.

Necessity for compliance with legal obligations: To meet regulatory and public interest obligations. In particular:

- To comply with applicable regulations and legislation.

4 Data retention

We retain personal data for so long as it is needed for the purposes for which it was collected or in line with legal and regulatory requirements or contractual arrangements.

5 Service providers

The Company may engage third party companies ("**Service Providers**") to facilitate the operation of our Services, assist in analyzing the usage of the Services, or perform related services, such as payment and the provision of IT infrastructure services. These third parties have access to the user's personal data only to the extent necessary to perform these tasks on behalf of the Company.

Type(s) of service providers who might access your personal data:

- Professional advisers that we use, such as accountant and lawyers

- Government or regulatory authorities
- Third parties who provide services such as, document processing and translation services, confidential paper shredding and/or disposal companies, software providers or IT systems, IT support services, document and information storage providers
- Third parties that are engaged in the course of your matter, such as counsel, mediators, banks and other payment providers, court, tax advisors or valuation experts

6 Data transfers

The Company and/or the Service Providers may transfer your personal data to and process it:

- In Switzerland
- In the European Union or the European Economic Area
- The United States

We may use Service Providers who are partly located in so-called third countries (outside the European Union or the European Economic Area) or process personal data there, i.e., countries whose level of data protection does not correspond to that of the European Union.

We safeguard your personal data per our contractual obligations and applicable data protection legislation when transferring data abroad.

Such safeguards may include:

- The transfer to countries that have been deemed to provide an adequate level of protection according to lists of countries published by the Federal Data Protection and Information Commissioner, as well as to countries where there is an adequacy decisions by the European Commission in place.
- Applying standard data protection model clauses, binding corporate rules or other standard contractual obligations that provide appropriate data protection.

7 Data disclosure

We may disclose your personal data in the good faith belief that such action is necessary:

- To comply with a legal obligation (i.e., if required by law or in response to valid requests by public authorities, such as a court or government agency).
- To protect the security of the Services and defend our rights or property.
- To prevent or investigate possible wrongdoing in connection with us.

- To defend ourselves against legal liability.

8 Data security

We take reasonable technical and organizational security measures that we deem appropriate to protect your stored data against manipulation, loss, or unauthorized third-party access. Our security measures are continually adapted to technological developments.

We also take internal data privacy very seriously. Our employees and the Service Providers that we retain are required to maintain secrecy and comply with applicable data protection legislation. In addition, they are granted access to personal data only insofar as this is necessary for them to carry out their respective tasks or mandate.

The security of your personal data is important to us but remember that no method of transmission over the Internet or electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your personal data, we cannot guarantee its absolute security. We recommend using antivirus software, a firewall, and other similar software to safeguard your system.

9 Your rights

You have the below data protection rights. To exercise these rights, you may contact the above address or send an e-mail to: team@intmax.io. Please note that we may ask you to verify your identity before responding to such requests.

Right of access: You have a right to request a copy of your personal data, which we will provide to you in an electronic form.

Right to amendment: You have the right to ask us to correct our records if you believe they contain incorrect or incomplete information about you.

Right to withdraw consent: If you have provided your consent to the processing of your personal data, you have the right to withdraw your consent with effect for the future. This includes cases where you wish to opt-out from marketing communications. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose(s) to which you initially consented unless there is another legal basis for processing. To stop receiving emails from us, please click on the 'unsubscribe' link in the email you received or contact us at team@intmax.io.

Right to erasure: You have the right to request that we delete your personal data when it is no longer necessary for the purposes for which it was collected or when it was unlawfully processed.

Right to restriction of processing: You have the right to request the restriction of our processing of your personal data where you believe it to be inaccurate, our processing is unlawful, or where we no

longer need to process it for the initial purpose, but where we are not able to delete it due to a legal obligation or because you do not want us to delete it.

Right to portability: You have the right to request that we transmit your personal data to another data controller in a standard format such as Excel, where this is data which you have provided to us and where we are processing it on the legal basis of your consent or to perform our contractual obligations.

Right to object to processing: Where the legal basis for our processing of your personal data is our legitimate interest, you have the right to object to such processing on grounds relating to your particular situation. We will abide by your request unless we have a compelling legal basis for the processing which overrides your interests or if we need to continue to process the personal data for the exercise or defense of a legal claim.

Right to lodge a complaint with a supervisory authority: You have the right of appeal to a data protection supervisory authority if you believe that the processing of your personal data violates data protection law. You are entitled to contact the relevant Supervisory Authority - in Switzerland, the Federal Data Protection and Information Commissioner, Feldeggweg 1 CH - 3003 Bern, info@edoeb.admin.ch. If you access the Website from one of the EU Member States, you can exercise this right, for example, before a supervisory authority in the Member State of your residence, your place of work, or the place of the alleged infringement.

10 Links to third-party apps and sites

Our Services may contain links to websites or apps that we do not operate. If you click a third-party link, you will be directed to that third party's site or app. We have no control over and assume no responsibility for the content, privacy policies or practices of any third-party sites or services.

11 Changes to this privacy policy

We may update our Privacy Policy from time to time. We, therefore, encourage you to review this Privacy Policy periodically for any changes.

Changes to this Privacy Policy are effective when they are posted on this page.

12 Contact us

If you have any questions about this Privacy Policy, do not hesitate to get in touch with us at: team@intmax.io.