

# Privacy Notice

---

**Controller:** Moneywheel Research Zrt. (“UltraFX”), 34 Munkás Str., 2120 Dunakeszi, Hungary. Company registration 13-10-041215 (Pest County Court); EU VAT HU23521050.

**Service:** Rental of virtual and dedicated servers with ultra-low-latency connectivity.

**Privacy contact:** [privacy@ultrafx.com](mailto:privacy@ultrafx.com)

**Data Protection Officer:** None appointed (a DPO Necessity Assessment supports this); please use [privacy@ultrafx.com](mailto:privacy@ultrafx.com) for any privacy matter.

**Version / effective date:** 4.0 / 1 June 2026

## At a glance

This summary highlights the key points; the full notice below gives the detail.

- We are **Moneywheel Research Zrt.** (“UltraFX”), a Hungarian company, and we are the controller for the personal data described here.
- We collect only what we need to open and run your account, take payment, issue invoices, provide support, keep our service secure, and meet our legal obligations.
- We do **not** carry out identity checks ourselves. For cryptocurrency payments, **Argos Identity** performs the check and we receive only a **pass or fail** result — we never see or store your identity documents.
- Your data is processed mainly in the **European Economic Area**. Any limited transfer abroad relies on a recognised legal safeguard.
- We keep account data for **5 years** after our relationship ends, and invoices for **8 years** as Hungarian law requires.
- You have rights over your data — including access, correction and deletion — and you can contact us or complain to a regulator at any time.

## 1. About this notice

This notice explains how Moneywheel Research Zrt. (“**we**”, “**us**” or “**UltraFX**”) collects and uses personal data when you visit our website, register and hold an account, pay for and use our server-rental service, contact our support team, or otherwise deal with us.

We are the **controller** of this personal data, which means we decide how and why it is processed. We do so in accordance with Regulation (EU) 2016/679 (the “**GDPR**”) and Hungarian Act CXII of 2011 on Informational Self-Determination and Freedom of Information. Because we are established in the European Union, we are not required to appoint a representative under Article 27 GDPR.

This notice should be read together with our **Terms of Service** and our **Cookie Policy**, which use the same defined terms.

### 1.1 What this notice does not cover

This notice does **not** apply to any content or data that you (or your own users) store, transmit or process on the servers you rent from us. Those servers are under your exclusive control: we do not access, monitor, manage, copy or back up what is on them, and you remain the controller of that data and responsible for it under applicable law.

It also does not govern the identity-verification step for cryptocurrency payments. That check is performed by **Argos Identity**, which acts as an independent controller for the identity data it collects and is responsible for it under its own privacy notice (<https://www.argosidentity.com>). We receive only the outcome of that check.

## 2. The personal data we collect

We are guided by the principle of data minimisation: we ask for and keep only what we genuinely need. The categories below reflect our actual processing.

Category	What it includes	Where it comes from
Account and contact data	Name, billing address, telephone number, email address, account identifier, and login credentials (passwords are stored only in hashed form)	You, when you register and manage your account
Payment-related data	The last four digits of your payment card, transaction references, amounts, currency, and payment status. We do <b>not</b> store full card numbers	Returned to us by our payment providers when you pay
Technical and usage data	IP address, browser type and version, operating system, the dates, times and duration of visits, pages viewed and links clicked, and device identifiers. On mobile devices, device type and identifier, operating system and browser	Collected automatically through the website and cookies
Customer-support and chat data	The content of the email and chat messages you exchange with our support team, including any attachments	You, when you contact support
Cryptocurrency verification result	A pass/fail result received from Argos Identity, together with the time of the result, linked to your account	Argos Identity, after you complete verification
Reports of misuse	Abuse complaints, take-down notices and lawful requests concerning the use of our infrastructure, and our records of handling them	The person or authority making the report

Providing your account, contact and payment data is necessary to enter into and perform our contract with you; if you do not provide it, we cannot open your account, deliver the service, take payment or issue an invoice. Other data — for example the content of a support message — is provided voluntarily.

## 3. Where we obtain your data

Most of the personal data we hold is provided **directly by you** when you register, pay, use the website or contact us. In addition:

- our **payment providers** return limited payment data to us (such as the last four digits of your card and the payment status) so that we can confirm and reconcile your payment;
- **Argos Identity** returns the **pass/fail** result of the cryptocurrency identity check (and nothing more);
- some **technical data** is collected automatically when you use the website, as described in our Cookie Policy; and
- **third parties or authorities** may provide us with information when they report suspected misuse of our infrastructure.

#### 4. How and why we use your data, and our legal basis

We use your personal data only for the purposes set out below, each of which has a clear legal basis under Article 6 GDPR.

Purpose	What this involves	Legal basis
Account and service	Registering you, opening and administering your account, and providing the server-rental service	Performance of a contract — Art. 6(1)(b)
Payments	Taking payment and handling refunds, chargebacks and disputes	Performance of a contract — Art. 6(1)(b); and compliance with a legal obligation (accounting, anti-fraud) — Art. 6(1)(c)
Cryptocurrency verification	Acting on the pass/fail result of the identity check for customers who pay in cryptocurrency	Compliance with applicable anti-money-laundering rules — Art. 6(1)(c) where they apply to us; otherwise the verification is a necessary precondition of that payment method — Art. 6(1)(b)/(f)
Invoicing and tax	Issuing invoices and reporting them to the Hungarian Tax Authority (NAV) through Billinggo	Compliance with a legal obligation — Art. 6(1)(c) (Act C of 2000 on Accounting; Act CXXVII of 2007 on VAT)
Security and prevention of misuse	Preventing fraud and abuse, keeping our infrastructure secure, and responding to reports about its use	Our legitimate interests in running a secure service free of misuse — Art. 6(1)(f); and legal obligation where applicable — Art. 6(1)(c)
Customer support	Responding to your queries and resolving technical and billing issues	Performance of a contract — Art. 6(1)(b); and our legitimate interest in improving service quality — Art. 6(1)(f)
Legal claims	Establishing, exercising or defending legal claims	Our legitimate interests in protecting our legal position — Art. 6(1)(f)

Where we rely on **legitimate interests**, we have weighed our interests against your rights and freedoms and concluded that the processing is proportionate. You may ask us for a summary of that assessment at any time by emailing [privacy@ultrafx.com](mailto:privacy@ultrafx.com). New service lines can be added to this table as further purposes, each with its own legal basis, without rewriting the rest of this notice.

## 5. Special-category data

We do **not** collect or process special-category personal data within the meaning of Article 9 GDPR — that is, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric data used to identify you, **health data**, or data about your sex life or sexual orientation.

The cryptocurrency identity check may involve such data (for example, the automated comparison of a photograph with an identity document). That processing is carried out by **Argos Identity as an independent controller**, under its own legal basis and privacy notice. We do not receive or store any of it; we receive only a pass/fail result.

## 6. Cookies and similar technologies

We use cookies and similar technologies to operate the website securely, to remember your preferences and — only with your consent — to understand how the site is used. Non-essential cookies are set only after you have consented through our cookie banner, and you can change or withdraw your choices at any time. Full details, including the cookies in use and how to manage them, are set out in our **Cookie Policy** at <https://www.ultrafx.com/en/cookie-policy>.

## 7. Service messages and marketing

We send you **service messages** that are necessary to operate the service you have engaged — for example account notifications, invoices, payment confirmations, security alerts, maintenance notices, support replies, and notices of changes to our terms or this notice. Because these are part of our contract with you, they are not a form of marketing and you cannot opt out of them while you hold an account.

We send **marketing messages**, such as a newsletter, only to people who have actively **opted in**, and every such message contains an unsubscribe link. You may withdraw your consent at any time, and you have the right under Article 21(2) GDPR to object to direct marketing at any time. We do **not** use purchased marketing lists, and we do **not** sell your personal data.

## 8. Who we share your data with

We share personal data only where it is necessary to operate the service and to meet our legal obligations. Our recipients fall into the following categories.

Recipient	Function	Role
Amazon Web Services (Frankfurt region)	Cloud hosting of our CRM	Processor
WHMCS	CRM and billing software	Processor
Stripe; PayPal	Card and e-wallet payment processing	Independent controller for their own anti-fraud and regulatory purposes; processor for executing the transaction
CoinsPaid / Dream Finance OÜ	Cryptocurrency payment processing	Independent controller
Argos Identity	Cryptocurrency identity verification	Independent controller
Bilingo	Invoicing and e-invoice submission to NAV	Processor
Zoho (EU instance)	Customer-support chat	Processor

Recipient	Function	Role
NAV, courts and other competent authorities	Statutory reporting and responses to lawful requests	Independent controller
Our professional advisers (lawyers, accountants, auditors)	Professional advice and audit	Independent controller
A buyer and its advisers in a corporate transaction	Due diligence and completion of a sale or reorganisation	Independent controller

Each of our **processors** acts only on our instructions under a contract that meets Article 28 GDPR. We do not share personal data with third-party advertising networks.

## 9. International data transfers

We process your personal data mainly within the **European Economic Area** (our CRM is hosted in the AWS Frankfurt region and our support chat runs on Zoho's EU instance). Where any limited transfer to a country outside the EEA takes place, we rely on a recognised safeguard under Chapter V GDPR — a European Commission **adequacy decision** (for example for the United Kingdom and the Republic of Korea), the **EU–US Data Privacy Framework** where the recipient is certified, or the Commission's **Standard Contractual Clauses** together with any additional measures that are appropriate. You may ask us for a summary of the safeguard that applies to a particular transfer by emailing [privacy@ultrafx.com](mailto:privacy@ultrafx.com).

## 10. How long we keep your data

We keep personal data only for as long as we need it for the purposes described in this notice, and then delete or anonymise it. Our standard periods are set out below.

Data	Retention period
Account and contact data	For the duration of our relationship and <b>5 years</b> afterwards, to allow us to defend legal claims
Invoices and the personal data on them	<b>8 years</b> from the end of the year of issue (Act C of 2000 on Accounting, §169)
Payment transaction data	As required by accounting and anti-money-laundering law
Customer-support and chat data	For the duration of our relationship and up to <b>5 years</b> afterwards
Cryptocurrency verification result	For the duration of our relationship and <b>5 years</b> afterwards (the underlying identity data is held by Argos under its own rules)
Records of misuse and lawful requests	<b>5 years</b> from closure, or longer where a specific legal hold applies

Where data is held in a back-up, it is deleted when that back-up is overwritten in our normal cycle. We do not currently use automated deletion; deletions are carried out on a documented manual schedule.

## 11. Your rights

Subject to the conditions and exceptions in the GDPR, you have the right to:

- **be informed** about how we use your data — which is the purpose of this notice;
- **access** your personal data and receive a copy of it;
- **correct** data that is inaccurate or incomplete;
- **erase** your data (the “right to be forgotten”), except where we must keep it to meet a legal obligation — such as our tax and accounting duties — or to defend legal claims;
- **restrict** our processing in certain circumstances;
- **object** to processing based on our legitimate interests, and at any time to processing for direct marketing;
- **data portability** — receive the data you provided to us in a structured, commonly used and machine-readable format; and
- **withdraw your consent** at any time where we rely on consent (for example for non-essential cookies or marketing), without affecting processing already carried out.

To exercise any of these rights, please contact [privacy@ultrafx.com](mailto:privacy@ultrafx.com) or write to us at our registered office. We will respond within one month; for complex or numerous requests we may extend this by up to two further months and will tell you if we do. To protect your data we may need to verify your identity before we act. There is normally no charge.

For the identity data collected during cryptocurrency verification, **Argos Identity** is the controller; please direct any request about that data to Argos, and we will help you reach them.

If you are concerned about how we handle your data, please contact us first so that we can try to resolve it. You also have the right to lodge a complaint with a supervisory authority — in Hungary, the **National Authority for Data Protection and Freedom of Information (NAIH)**, H-1055 Budapest, Falk Miksa u. 9-11; +36-1-391-1400; [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu); [www.naih.hu](http://www.naih.hu) — or with the authority in the country where you live or work.

## 12. Automated decision-making and profiling

We do not make decisions about you based solely on automated processing that produce legal effects concerning you or otherwise similarly significantly affect you. The automated elements of cryptocurrency identity verification are carried out by **Argos Identity** as an independent controller, under its own privacy notice and rights regime. If this position changes, we will update this notice and explain the logic involved, the significance of the processing and the rights available to you.

## 13. How we keep your data secure

We apply technical and organisational measures appropriate to the risk of our processing. Our **current** measures include:

- password protection for access to customer accounts and rented servers, with passwords stored only in hashed form;
- limiting access to our systems to authorised personnel;
- hosting our CRM in the AWS Frankfurt region, relying on AWS’s infrastructure and physical-security controls; and
- protecting connections to our website in transit using TLS.

We are progressively **strengthening** these measures — including introducing multi-factor authentication, role-based access control and access logging — as set out in our internal Information Security Policy. These should not be read as already fully in place. We have not pursued ISO/IEC 27001 (or any equivalent) certification at this stage and make no such claim.

#### 14. Children

Our services are intended for, and may only be used by, adults and legal entities. They are not directed at children, and we do not knowingly collect the personal data of anyone under the age of 18. If you believe a minor has provided us with personal data, please contact us so that we can delete it.

#### 15. Reports of misuse and lawful requests

As an infrastructure provider, we may receive **abuse complaints** and take-down notices about how our infrastructure is being used, and **lawful requests** from courts, regulators (including NAV), law-enforcement agencies and other competent authorities. We assess and respond to such matters in accordance with applicable law and, where appropriate, after taking legal advice. Where necessary, we may investigate, and we may suspend or terminate an account.

#### 16. Changes, language and how to contact us

We may update this notice from time to time. Where a change is material, we will communicate it in advance through our website or by contacting you directly; the version number and effective date above show the current version.

The authoritative version of this notice is in **English**; a Hungarian-language version is available on request. If there is any inconsistency between the two, the English version prevails.

For any question about this notice or about how we handle your personal data, please contact us at **privacy@ultrafx.com** or by post at Moneywheel Research Zrt., 34 Munkás Str., 2120 Dunakeszi, Hungary.