

Privacy Notice

This notice has been prepared under Articles 13 and 14 of Regulation (EU) 2016/679 (GDPR) and Hungarian Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (Infotv.).

1. Who and what does this cover? Two roles

PrinterMS holds two kinds of data, governed by different rules:

- 1. What we process about you:** your account, your organisation's registration and subscription payment data, correspondence with us, website visits and device support requests. **This notice** applies to these; the controller is Sziráki Márton e.v.
- 2. What the subscribing organisation stores in PrinterMS:** a printer leasing company's customers, contracts, invoices, meter readings and issue reports. **The subscriber is the controller** of this data; we act as a **processor** on its instructions under the [Data Processing Agreement](#). If you appear in the system as a subscriber's customer, you should primarily exercise your rights with that subscriber; if you contact us, we forward your request to it.

The public QR issue reporting interface displays a separate, short notice. Cookies are covered by the [Cookie Notice](#).

2. The controller

Controller	Sziráki Márton e.v.
Registered office	2141 Csömör, Középhegy utca 14.
Registration number	62576336
Tax number	92221338-2-33
Privacy contact	privacy@printerms.com
Data protection officer	none (not required under GDPR Article 37); you can contact us directly at the address above

3. What data do we process, why and for how long?

3.1 Account and sign-in

Data	Purpose	Legal basis	Retention
name, email address, role, organisation membership	providing the service, identification, permission management	performance of a contract, GDPR Article 6(1)(b)	for as long as the account exists; a removed organisation member's authentication account remains disabled until the organisation is deleted; on organisation deletion, everything is deleted after the 30-day grace period
password verification data and two-factor authentication secret (managed by Amazon Cognito in Ireland; we do not store the password)	secure sign-in	GDPR Article 6(1)(b)	for as long as the account exists

Data	Purpose	Legal basis	Retention
confirmation and password reset codes, temporary password on invitation	account creation and recovery	GDPR Article 6(1)(b)	codes are valid for a few minutes, temporary passwords for a few days; we do not store email content
session: identifier hash, interface, authentication level and timestamps (without IP address or browser identifier)	maintaining sign-in and allowing revocation	GDPR Article 6(1)(b)	expires after 7 days of inactivity, or after 30 days at the latest; the record is deleted 90 days after expiry or revocation
evidence of contract acceptance: email address, identifiers and content hashes of accepted documents, exact declaration text and timestamp, IP address, browser identifier	proving the conclusion and content of the contract, defending legal claims	GDPR Article 6(1)(b) and (f)	unused receipt: 30 days; evidence linked to a contract: for the term of the contract and 5 years thereafter

3.2 Organisation details and subscription payments

Data	Purpose	Legal basis	Retention
company name, registered office, tax number, company registration number, representative's name, contact and billing email address, phone number, bank account details	concluding the contract, communication, subscription billing	GDPR Article 6(1)(b)	until the contract ends
Stripe customer, subscription and transaction identifiers, payment method and status, billing address	payment by card or bank transfer, subscription management, payment reminders	GDPR Article 6(1)(b); Stripe is an independent controller for its own fraud prevention and statutory purposes	for the term of the contract and according to Stripe's own retention obligations
data in invoices issued by us	accounting obligations	legal obligation, GDPR Article 6(1)(c); section 169 of the Hungarian Accounting Act	8 years

We do not receive your card number or security code; Stripe handles these. The VAT invoice for our fees is issued through our own Billing account.

3.3 Invited users

If your organisation invites you to PrinterMS, we receive your email address and role **from that organisation**. Purpose: delivering the invitation, creating the account and managing access. Legal basis: the organisation's and PrinterMS's legitimate interest in providing the service securely (GDPR Article 6(1)(f)). If you do not accept the invitation, the data is deleted when the invitation expires.

3.4 Customer portal users

If a subscriber invites you to its customer portal, we receive your email address and name **from that subscriber**. The subscriber is the controller of data viewed and submitted in the portal (printer fleet, meter readings, invoices, issue reports). We are responsible as an independent controller for sign-in security (single-use email code, session, rate limiting), based on legitimate interest (GDPR Article 6(1)(f)). When your access ends, we delete your authentication account, and session records after 90 days.

3.5 Support and feedback

Data	Purpose	Legal basis	Retention
name, email address, enquiry content	answering the question, troubleshooting	legitimate interest, GDPR Article 6(1)(f); for contractual matters, Article 6(1)(b)	3 years after the enquiry is closed
voluntary exit survey on cancellation or account deletion: reason for cancellation, suggestion, comment, plan and approximate number of printers (without name or email address)	improving the service	legitimate interest, GDPR Article 6(1)(f)	13 months

We access your organisation's data stored in PrinterMS **only at your request and to the extent necessary for troubleshooting**.

3.6 Device support requests

If you request support for a printer or your organisation joins the device support programme, the DCA Agent performs a single walk of the printer's technical data (serial number, network and email addresses, hostnames and longer text are redacted within the local network). You may also attach a photograph or PDF to the request.

Data	Purpose	Legal basis	Retention
redacted walk, attached file (if it shows personal data), requesting user's identifier and declaration timestamp	improving printer support; a model-level compatibility list that does not allow identification	legitimate interest, GDPR Article 6(1)(f) (following your request or choice to join the programme)	walk and attached file: 365 days; request result: until the organisation is deleted

We may also use AI-based development tools for analysis, but they receive only the redacted walk, without the attached file or user, customer or device identifiers.

3.7 Measuring website and application usage

The public website uses Cloudflare's cookie-free, aggregate traffic measurement. PostHog product analytics and limited Google Analytics 4 measurement start **only with your prior consent** (GDPR Article 6(1)(a)). We process normalised paths, campaign parameters, pseudonymous user and organisation identifiers, role, plan and approved events. We do not send names, email addresses, tax numbers, serial numbers, customer or invoice data, form content, searches or filenames.

We do not send user or organisation identifiers to Google Analytics and do not enable advertising features; individual data is retained there for 2 months. Session replay, which requires separate permission, runs on an approximately 5% sample; all inputs and user text are masked, and sensitive pages are excluded. We retain raw events for 12 months, replays for 30 days and anonymous aggregates for no more than 24 months. We retain your choice for 1 year and evidence of consent or withdrawal for 5 years. Consent may be withdrawn at any time without affecting the lawfulness of earlier processing.

We do not send newsletters or promotional emails. Transactional, authentication, billing, security and support messages necessary for the service are not direct marketing messages.

3.8 Abuse prevention

We use IP-based rate limiting on PrinterMS endpoints to prevent abuse, based on legitimate interest (GDPR Article 6(1)(f)). On authentication and public endpoints (registration, password reset, customer portal sign-in, two-factor authentication reset, QR issue reporting), we retain the IP address for no more than 48 hours (daily deletion removes records older than 24 hours); on other endpoints, the counter exists only in server memory for a few minutes. We do not save the IP address with the QR issue report.

3.9 Logs

We log operational and security events for security and accountability (legitimate interest, GDPR Article 6(1)(f); for privacy operation logs, legal obligation under Article 6(1)(c)). The application's own request log does not contain IP addresses. Retention: cloud platform request logs (IP address, browser identifier, path): 30 days; application system logs: 90 days, unresolved errors: 1 year; cloud provider administrative and authentication audit logs: no more than 400 days; operational notification email delivery records: 90 days; sending records for our subscription invoices and account notifications: until the organisation is deleted; privacy operation and document acceptance logs: 5 years.

3.10 Is providing data mandatory?

Providing the data under sections 3.1 and 3.2 is a condition of concluding and performing the contract: without it, we cannot create an account or provide the service. All other data is voluntary; not providing it affects only the relevant feature (for example, attaching a photograph to a support request).

4. Who has access to the data?

We do not sell your data or share it for marketing purposes. We engage contracted processors to operate the service:

Processor	Task	Location
Google Cloud EMEA Limited	database, file storage, application runtime, AI-based invoice processing; privacy@ and support@ mailboxes (Google Workspace)	EU (Belgium); mailboxes on global infrastructure
Amazon Web Services EMEA SARL	sign-in, sending and receiving email	EU (Ireland)
Cloudflare, Inc.	website delivery, CDN, real-time signals	global edge network
PostHog Cloud EU, Google Ireland Limited (Google Analytics 4)	consent-based analytics	EU (Frankfurt) and global, respectively
Stripe Payments Europe, Limited	subscription payments and management	Ireland and Stripe's global network
Billingo Technologies Zrt.	issuing the VAT invoice for our fees	Hungary
Supabase Pte. Ltd. (being phased out)	only a sealed copy of the state before 25 September 2026, to be deleted by 30 November 2026 at the latest	EU (Frankfurt)

The full, current list with safeguards is in the [Subprocessor Register](#). We disclose data to authorities only in response to requests based on law.

5. Transfers outside the EU

We primarily store data within the EU. Transfers outside the EU may involve Cloudflare (USA), AWS and Google's global support operations, Google Workspace mailboxes, Google Analytics, Stripe and Supabase, which is being phased out (Singapore, as the contracting entity). In each case, safeguards are the European Commission's Standard Contractual Clauses (SCCs) or certification under the EU-US Data Privacy Framework, as applicable; details are in the [Subprocessor Register](#). Copies of the safeguards are available on request.

6. Automated decision-making and artificial intelligence

We do not make decisions based solely on automated processing that have legal effects on you. We use Google Vertex AI (Gemini) through an EU endpoint to extract data from supplier invoices. The result is always a proposal

awaiting review and approval by the user. Google does not use uploaded documents to train models without our instructions; the service's technical operation may involve short-term caching, so we do not promise zero retention.

7. Your rights

You can exercise your rights free of charge at privacy@printerms.com; we respond within 1 month at the latest (for complex requests, this may be extended by no more than 2 months, and we notify you).

- **Access** (Article 15): information and a copy of your data.
- **Rectification** (Article 16): you can correct most account details yourself in the interface.
- **Erasure** (Article 17): except data subject to statutory retention obligations (such as invoices).
- **Restriction** (Article 18).
- **Data portability** (Article 20): we provide your contract-based data in a machine-readable format; the main data categories can also be exported from the interface ([Data portability](#)).
- **Withdrawal of consent** (Article 7(3)).

Objection (Article 21). You may object at any time, on grounds relating to your particular situation, to processing based on legitimate interest (section 3.1: acceptance evidence; sections 3.3, 3.4, 3.5, 3.6, 3.8 and 3.9). We then continue processing only where there are compelling legitimate grounds.

8. Remedies

- **Hungarian National Authority for Data Protection and Freedom of Information (NAIH):** 1055 Budapest, Falk Miksa utca 9-11.; postal address: 1363 Budapest, Pf. 9.; phone: +36 (1) 391-1400; email: ugyfelszolgalat@naih.hu; www.naih.hu.
- **Courts:** under section 23 of the Infotv.; proceedings may also be brought before the regional court for your permanent or temporary place of residence.

Within five years after a data subject's death, their rights may be exercised by a person authorised by them during their lifetime or, in the absence of such a person, a close relative under the Hungarian Civil Code (section 25 of the Infotv.).

Please raise the issue with us first: this is the quickest way for us to help.

9. Data security

The security measures, backup arrangements and retention periods for subscriber data are described on the [Data security and retention](#) page.

10. Children

PrinterMS is for business use only; we do not provide services to people under 16 and do not intentionally process their data.

11. Changes

We update this notice when our processing changes; the latest update date appears at the top. We also notify you of material changes by email or in the application.