

Your data. Protected.

How PrinterMS protects your company's data

Version 1.1 · October 2026 · printerms.com/en/security

Your customer list, page prices, contracts and margins: PrinterMS holds your company's most valuable business knowledge. We know exactly what you entrust to us, and this information sheet explains openly how we look after it. It is not a technical document: it sets out the principles and protections that safeguard your data, so you can make an informed decision.

THE ESSENTIALS

Every organisation's data lives in its own private space: other PrinterMS customers, including your competitors, can never see any of it. Your data is encrypted in transit and at rest, in a Belgian data centre in the European Union, with automatic daily backups. You control access within your team, and PrinterMS staff only access your data at your request. You can take all your data with you at any time: there is no data lock-in or notice period.

1. What you entrust to us

A leasing company's real wealth is its records: who your customers are, what you charge per page, when contracts expire and how much margin you make. That knowledge takes years, often decades, to build. It would be worth a fortune to a competitor, so we protect it accordingly.

What you store in the system

- printer fleet, contracts and meter readings
- customer and supplier details
- prices, charges, revenue and invoices
- service history and inventory

What we never do with your data

- sell it or pass it on to anyone
- analyse it for anyone else's benefit or turn it into a product
- look through it, except at your request to investigate an issue
- hold it hostage: you can export it and request deletion at any time

2. Data isolated by organisation

Many companies use PrinterMS, but every organisation's data lives in its own private space. Isolation is enforced at the deepest database layer for user requests, and background processes always explicitly filter for your organisation. The boundary would still hold if someone made a mistake in the interface, and we regularly test it from an attacker's perspective too. Other PrinterMS customers, including your closest competitors, cannot see any of your data through any route.

3. Encryption, storage and backups

- **Bank-grade encryption.** Traffic between your browser and the system, stored data and backups are encrypted.
- **Separately protected keys.** Billingo and Számlázz.hu integration keys have a separate layer of encryption that keeps them isolated even from the rest of the system.
- **EU data centres.** Your database, files and backups are stored in the European Union: the database and files in Belgium, and daily backups in EU data centres, under the full protection of the GDPR.
- **Daily backups.** The database is backed up automatically each day with encryption, and can be restored to any point in the preceding week, so a failure cannot wipe out your company's records.

4. Access: you decide who sees what

- **Roles within your team.** The owner role can see everything, while technicians can only access the data needed for daily work: never financial data, prices or margins.
- **Stronger sign-in.** You can protect accounts with two-step verification, so a leaked password alone is not enough to sign in. The system automatically slows and blocks repeated login attacks.
- **You manage access.** You invite team members and can remove them at any time; their access ends immediately.
- **We leave your data alone.** PrinterMS staff do not look through your data. We only access it at your request to investigate an issue.

5. Ongoing protection

- **Checked releases.** Every change passes automated security checks before reaching production.
- **Continuous scanning.** We continually scan system components for known vulnerabilities.
- **An attacker's perspective too.** We regularly examine the whole system from an attacker's perspective, from sign-in to billing. We do not wait for someone else to find a weakness.

6. The printer monitoring agent (DCA) at a glance

The data collector installed at customer sites only makes outbound connections, only reads from printers, and never sees documents, print jobs or scanned material. It handles technical printer data (meter readings, toner levels and device status) and the network data needed for its own operation. If your customer's IT administrator has questions, you can give them a ready-made answer: the detailed technical information sheet is available from printerms.com (PDF).

7. Your data, your decision

You can download your main data categories as an Excel workbook at any time, with one click. Additional data is provided in machine-readable form on request. There is no notice period or data lock-in: we want you to stay because the product is good, rather than because you cannot leave. If you decide to leave, we permanently delete your organisation's service data after the 30-day recovery period; only data that must be retained by law remains for the necessary period. We operate under the GDPR; details are available in the [privacy notice](#).

8. Frequently asked questions

Can another PrinterMS customer see my data?

No, under no circumstances. Every organisation's data lives in its own private space, and isolation is enforced at the deepest database layer, on every query. We regularly test the boundary from an attacker's perspective too.

Can PrinterMS see anything my customers print?

No. The system only handles technical printer data: meter readings, toner levels and device status. Neither the agent nor the cloud can access documents, print jobs or scanned material.

Who within my company can access my data?

Only the people you invite, and only as much as they need for their work. Technicians never see financial data, prices or margins. Sign-in can be strengthened with two-step verification, and you can remove team members at any time.

What happens to my data if I leave?

First, you download your main data categories as an Excel workbook with one click. At the end of the 30-day recovery period, we permanently delete your organisation's service data under the GDPR; only accounting records and legal evidence subject to mandatory retention remain for the necessary period. The data is yours: it works in our system, but belongs to you.

9. Questions and contact

If you have any further questions, email support@printerms.com: the development team replies directly. The latest version of this information is always available at printerms.com/en/security. Details of data processing are set out in the [privacy notice](#).

PrinterMS · printerms.com · Data security information, version 1.1, October 2026. This document reflects the position at the time of publication.