

Data security and retention

This page explains where we store Subscriber Data, how we protect it and how long we retain it. It is incorporated by reference into the [Data Processing Agreement](#) and also constitutes the disclosure required by Article 28 of Regulation (EU) 2023/2854 (the Data Act).

How this may change: we update security measures as technology develops, without reducing the level of protection. We shorten a retention period only after publishing the change on this page under "Planned changes" and notifying Subscribers by email at least 30 days in advance; an extension is possible only through an amendment under section 16.3 of the Terms of Service. Retention periods for processing for our own purposes are set out in the [Privacy Notice](#).

1. Where the data is stored

Service	Provider	Location and jurisdiction
database, file storage, application and background processes	Google Cloud EMEA Limited (Cloud SQL, Cloud Storage, Cloud Run and related services)	Belgium (europe-west1); database backups in multi-region storage within the EU; contracting entity: Ireland
AI-based invoice data extraction	Google Cloud EMEA Limited (Vertex AI)	Google data centres within the EU, through an EU endpoint
sign-in, two-factor authentication, sending and receiving email	Amazon Web Services EMEA SARL (Cognito, SES, SNS, SQS)	Ireland (eu-west-1); contracting entity: Luxembourg
website, CDN, DNS, real-time update signals	Cloudflare, Inc.	global edge network; storage for real-time signals is restricted to EU jurisdiction; contracting entity: USA
privacy and support mailboxes	Google Cloud EMEA Limited (Google Workspace)	global infrastructure

The providers' roles, the data they process and the transfer safeguards are detailed in the [Subprocessor Register](#).

Being phased out. The former database, authentication and storage provider (Supabase Pte. Ltd., Frankfurt) has not processed live data since 25 September 2026; the sealed copy of the state before the migration and the disabled accounts remaining in the Google Identity Platform test environment will be deleted by **30 November 2026** at the latest.

Agent installation and update packages are available from GitHub release storage, usually through Cloudflare at agent.printerms.com. This route does not transmit Subscriber Data.

2. Protection against access by authorities in third countries

- We select a primary storage and processing region within the European Union wherever the service allows this.
- We use data processing agreements, the European Commission's Standard Contractual Clauses and the EU-US Data Privacy Framework, as applicable.
- We use encryption in transit and at rest, least privilege and logged access.
- In response to a request based on law, we disclose only the minimum data required, notify the Subscriber unless prohibited by law, and challenge requests that are manifestly unlawful or disproportionate.

3. Security measures

Area	Measure
Tenant isolation	organisation identifier on every record; user requests run with row-level security (RLS) on all production tables; background processes use explicit organisation filters; organisation resolution for public interfaces takes place on the server
Access control	role-based permissions (technicians cannot access financial data); customer portal users see only data belonging to their assigned customer; platform-level administrative operations are logged
Authentication	managed authentication service (we do not store the password); passwords of at least 12 characters; two-factor authentication enforceable at organisation level; single-use email codes in the customer portal; short-lived access tokens; HttpOnly / Secure session cookie with CSRF protection (7 days of inactivity, 30 days at most); all sessions revoked on password reset
Encryption	TLS for all transfers; AES-256-GCM encryption of integration keys and device tokens, with key rotation; encryption of stored data and backups
Network and application	database accessible only through a private network with identity-based authentication; rate limiting; signature-verified webhooks; strict security headers (CSP, HSTS)
Development	mandatory automated tests, secret-leak and vulnerability checks before every production deployment; separate test and production environments; signed Agent releases
Logging	security and privacy operation event logs (export, deletion); cloud provider audit logs
Personnel	confidentiality obligations; we access the Subscriber's data only on request for troubleshooting; human database access only through individual, logged, read-only connections
Data minimisation	the QR reporter's IP address is not attached to the report; session records do not contain IP addresses; real-time signals carry only opaque identifiers; the Agent removes identifiers from device-support walks locally
Incident handling	documented procedures, with notification under section 7 of the Data Processing Agreement

4. Backups

An encrypted database backup is created daily within the EU; point-in-time recovery (PITR) is available for the preceding 7 days. A full encrypted export is created weekly and retained for no more than 35 days, or **42 days** at most including the recoverability of deleted objects. A temporary copy is created for the quarterly recovery test and deleted when the test ends. Deleted data is also removed from backups within these periods. The database runs in a single zone; in the event of a zone failure, we restore it from a backup.

5. Retention periods

Business records: for as long as the account exists. Customers, suppliers, sites, printers, contracts and tariffs, meter readings (including DCA meter history), sales and supplier invoice data and sales invoice PDFs, revenue data, parts and stock, service logs, signed work sheets and Users. The Subscriber may delete these earlier.

Technical and operational data: deleted automatically on expiry.

Data	Retention
content of processed meter reading emails	30 days
meter reading emails that cannot be matched or await manual intervention	90 days
email processing log (sender, subject, result)	180 days

Data	Retention
uploaded supplier invoice file (the extracted data is retained)	60 days
closed QR issue report	180 days from closure (open reports until closure or deletion)
DCA submission packages	30 days
DCA device status history	30 days
DCA supply level history	90 days
DCA intraday meter samples (the daily meter reading is retained as a business record)	90 days
closed DCA alerts	180 days from closure (active alerts and the latest status are retained)
identifying data of unapproved, pending Monitor devices	30 days
device-support walk and its attached photograph or PDF	365 days
meter reconciliation results (Agent and independent reading)	400 days
trial rule results	30 days
notification email delivery records	90 days
data export workbook	72 hours (the request record: 30 days)
records of expired or revoked sessions	90 days
application system logs	90 days (unresolved errors: 365 days)
cloud platform request logs (IP address, browser identifier)	30 days
real-time update signals (opaque identifiers only)	7 days
failed email delivery queue	no more than 14 days

Deletion after termination of the contract and account deletion is governed by section 9.4 of the Data Processing Agreement; backups are governed by section 4 of this page.

6. Planned changes

Effective 30 November 2026. We are shortening the retention periods below and introducing a retention period for data not yet listed in the table. Business records (section 5) are not affected.

Data	Currently	From 30 November 2026
DCA submission packages	30 days	7 days after successful processing; a package that cannot be processed: 30 days

Data	Currently	From 30 November 2026
real-time update signals (opaque identifiers only)	7 days	until delivery; an undeliverable signal: 7 days
unfinished data import (an import awaiting review or failed, with its uploaded file and preview rows)	for the lifetime of the account	90 days from the last change
organization access and permission log, client portal access log	for the lifetime of the account	400 days

The data of a completed import is kept as a business record. After the change these rows move to the table in section 5.

Contact: **privacy@printerms.com**.