

# Data Processing Agreement

## Agreement under Article 28(3) of the GDPR

This agreement forms part of the [Terms of Service](#), is concluded by accepting them without a separate signature, and is valid in electronic form (GDPR Article 28(9)). For the processing of personal data, it takes precedence over the other provisions of the Terms of Service. The definitions in the Terms of Service also apply here.

## 1. Parties and roles

1.1 **Controller:** the Subscriber, in respect of personal data within Subscriber Data. **Processor:** Sziráki Márton e.v. (2141 Csömör, Középhegy utca 14.; tax number: 92221338-2-33), referred to as the Provider.

1.2 This agreement does not cover processing for which the Provider itself is the controller (subscriber account and subscription billing data, website visits, abuse prevention, and device support development under section 2 of the DCA Agent terms). These are covered by the [Privacy Notice](#).

1.3 **Services connected by the Subscriber** (for example, Billingo and Számlázz.hu) have a contract with the Subscriber and are not the Provider's subprocessors. The Subscriber instructs the Provider to send data to and receive data from these services according to its settings. Further processing of the received data is governed by the relationship between the Subscriber and the relevant service provider.

## 2. Subject matter of processing

The subject matter, nature, purpose and duration of processing, and the categories of data subjects and data, are set out in the Appendix at the end of this agreement.

## 3. The Provider's obligations

The Provider:

- a) processes Subscriber Data **only on documented instructions from the Subscriber**. Instructions include the contract, use and configuration of Service features (including declarations made in the interface, allocation of customer portal access and connection of integrations), and the Subscriber's written instructions. Transfers to a third country also take place only on instructions or where required by EU or Member State law; the Provider gives prior notice of such a requirement unless the law prohibits this on important grounds of public interest;
- b) informs the Subscriber without delay if, in its opinion, an instruction infringes the law, and may suspend execution of a manifestly unlawful instruction;
- c) ensures that persons with access to the data are bound by confidentiality obligations; its staff access the Subscriber's data only at the Subscriber's request, for troubleshooting and to the extent necessary;
- d) implements the technical and organisational measures described on the [Data security and retention](#) page (GDPR Article 32). It may update these as technology develops, **but must not reduce the level of protection**;
- e) provides assistance under sections 5-8, deletes or returns data under section 9, and allows audits under section 10;
- f) maintains the records required by GDPR Article 30(2).

## 4. Transfers to third countries

---

4.1 The Provider primarily stores and processes Subscriber Data within the European Union. Processing involving a third country takes place only with the subprocessors listed in the Subprocessor Register, using the safeguards specified there (the European Commission's Standard Contractual Clauses or certification under the EU-US Data Privacy Framework, as applicable).

4.2 If a safeguard ceases to be valid, the Provider applies another safeguard or suspends the affected processing without delay and notifies the Subscriber.

## 5. Data subject requests

---

5.1 The Provider assists the Subscriber in responding to data subject requests using means appropriate to the nature of processing: the Service's search, export and deletion features, or [privacy@printerms.com](mailto:privacy@printerms.com) for individual cases.

5.2 If a data subject contacts the Provider directly with a request concerning Subscriber Data, the Provider forwards it to the Subscriber within 5 working days at the latest and does not provide a substantive response unless instructed by the Subscriber or required by law.

## 6. Subprocessors

---

6.1 The Subscriber gives general authorisation to use the subprocessors listed in the [Subprocessor Register](#). The register forms part of this agreement.

6.2 The Provider notifies the Subscriber at least **30 days** before appointing or replacing a subprocessor, by email and by updating the register. If a replacement is urgent to maintain the Service's security or continuity and processing is transferred to a subprocessor already listed in the register, the Provider may act without waiting for the 30-day period, but still sends the notification before the replacement; the Subscriber retains its rights under section 6.3.

6.3 Within 30 days of notification, the Subscriber may object on data protection grounds, stating its reasons. The parties then consult. If no reasonable solution is found, the Subscriber may terminate the affected part of the Service or the contract free of charge; the pro-rata portion of unused prepaid fees is refunded.

6.4 The Provider imposes data protection obligations at least equivalent to those in this agreement on subprocessors and is liable for their performance as if it had acted itself (GDPR Article 28(4)).

6.5 When a subprocessor is phased out, the Provider ensures that Subscriber Data remaining with it is deleted within no more than 90 days of the phase-out; the register continues to list the subprocessor until deletion.

## 7. Personal data breach

---

7.1 The Provider notifies the Subscriber of a personal data breach affecting Subscriber Data without undue delay, preferably within 48 hours of becoming aware of it.

7.2 The notification, which may be provided in stages, includes the nature of the breach, the affected categories of data and data subjects, the likely consequences, measures taken and planned, and a contact person. The Provider documents the breach and cooperates with the Subscriber in meeting its obligations under GDPR Articles 33-34. The Subscriber decides on notification to the authority and data subjects. Notification does not constitute an admission of liability.

## 8. Assistance with GDPR Articles 32-36

---

Using the information available to it, the Provider assists the Subscriber with its obligations concerning data security, breach handling, data protection impact assessments and prior consultation; this agreement and the Data

security and retention page may also be used for this purpose.

## 9. Retention, return and deletion

---

**9.1 Business records.** The Provider retains the Subscriber's business records (customers, suppliers, sites, printers, contracts and tariffs, meter readings, invoices and revenue data, parts and stock, service logs, signed work sheets and Users) for as long as the account exists, unless the Subscriber deletes them earlier.

**9.2 Technical and operational data.** The Provider retains other data (such as raw emails and device submissions, device status, supply level and alert history, closed issue reports, uploaded source files and logs) for no longer than the periods set out on the [Data security and retention](#) page, then deletes it automatically. The Provider publishes a shortened retention period on that page and notifies Subscribers by email at least 30 days before it takes effect; an extension constitutes an amendment under section 16.3 of the Terms of Service.

**9.3 Plan changes.** Changing the Plan, cancelling a paid feature or stopping monitoring of a printer does not end processing; data already collected remains part of the active account.

**9.4 Termination and account deletion.** After the contract ends, the Subscriber may export its data for at least 30 days (section 15.4 of the Terms of Service). After that period, or after the 30-day grace period for account deletion initiated in the interface, the Provider **permanently deletes** Subscriber Data, unless EU or Member State law requires further retention.

**9.5 Backups.** Deleted data is removed from backups within the backup retention period specified on the Data security and retention page. The Provider accesses backups only for recovery and to verify recovery; after restoration, it reapplies previous deletions without delay.

**9.6** On request, the Provider confirms deletion in writing.

## 10. Audits

---

**10.1** To demonstrate compliance, the Provider makes the necessary information available, including the content of the Data security and retention page, the Subprocessor Register and infrastructure providers' certifications.

**10.2** If this is insufficient, the Subscriber may conduct an audit once per calendar year, with at least 30 days' notice, subject to confidentiality, either itself or through an auditor who is not a competitor of the Provider, in the manner least disruptive to the Provider's operations and at its own expense. Other subscribers' data and the Provider's trade secrets must not be disclosed. The once-a-year limit does not apply following a regulatory investigation or a confirmed breach.

## 11. Liability

---

Claims arising from this agreement are governed by the liability provisions of the Terms of Service unless mandatory law requires otherwise. The limit under section 9.2 of the Terms of Service, but not the exclusion under section 9.3, applies to recourse claims between the parties under GDPR Article 82(5) based on their actual respective responsibility. This does not affect data subjects' claims under GDPR Article 82.

## 12. Final provisions

---

**12.1** This agreement applies for the term of the contract and the period specified in section 9.

**12.2** Amendments are governed by section 16 of the Terms of Service; updates to the Subprocessor Register by section 6; and updates to the Data security and retention page by sections 3(d) and 9.2. Changes affecting mandatory GDPR provisions take effect in accordance with the law.

## Appendix: description of processing

---

**Subject matter and duration:** providing the PrinterMS Service to the Subscriber for the term of the contract and until deletion under section 9.

**Nature:** storage, organisation, retrieval and display; collection of data from the Subscriber's devices (DCA Agent) and email reports; calculation (charges and revenue); transmission on the Subscriber's instructions (Invoicing Providers, notification emails, customer portal); AI-based data extraction with human approval; backup and deletion.

**Purpose:** providing the Service under the Terms of Service and the Documentation.

**Categories of data subjects:**

- contacts at the Subscriber's customers and suppliers, and its sole trader customers and suppliers;
- the Subscriber's Users, in respect of their activity recorded in the Service;
- customer portal users invited by the Subscriber;
- people submitting reports through the public QR issue reporting interface;
- people signing service work sheets;
- senders of device emails and other persons recorded by the Subscriber in free-text fields.

**Categories of personal data:**

- identification and contact data (name, email address, phone number, address, tax number);
- contract, charge and invoice data, and the content of uploaded documents (such as supplier invoices);
- issue reports and customer portal activity;
- signed work sheets: signer's name, normalised signature stroke (without a biometric template), declaration text and timestamp;
- device and network data that may constitute personal data depending on the context (IP address, hostname, device messages);
- email content and metadata, free-text fields and log data.

**Special category data:** the Service is not intended to process special category data; the Subscriber must not enter such data.

**Retention, security measures and subprocessors:** as set out in section 9, the [Data security and retention](#) page and the [Subprocessor Register](#).