

Data processing agreement

Version 2026-11. This agreement forms part of every service agreement with POISE AB and governs how POISE processes personal data on the customer's behalf under Article 28 of the GDPR.

1. Parties and application

This agreement is between the customer (the "controller") and POISE AB, company reg. no. 556773-0923, Brunnsgatan 9, 172 68 Sundbyberg, Sweden (the "processor"), and forms part of the customer's service agreement. It governs the processor's processing of personal data on the customer's behalf under Article 28 of Regulation (EU) 2016/679.

2. Nature and purpose

The subject matter, duration, nature, purpose, types of personal data and categories of data subjects are set out in Annex 1 for the service(s) the customer buys.

3. Controller obligations

The customer is responsible for the lawful basis of the processing, for the lawfulness of its instructions and for informing data subjects. The customer is responsible for its own agreements with platform providers (for example Microsoft) where the processor administers the customer's own licences.

4. Processor obligations

The processor shall

- a. process personal data only on the customer's documented instructions, the service agreement and this agreement constituting such instructions;
- b. ensure that persons with access to the data are bound by confidentiality;
- c. implement the technical and organisational measures in section 6;
- d. assist the customer in responding to data-subject requests, within five working days of receiving the request;
- e. assist with data protection impact assessments and prior consultations;
- f. notify the customer without undue delay, and no later than 48 hours after becoming aware of a personal data breach concerning the customer's data, with the information then available;
- g. delete or return all personal data at the end of the service, per section 9;
- h. make available the information necessary to demonstrate compliance and allow audits per section 8;
- i. inform the customer immediately if it considers an instruction to infringe data protection law;
- j. where the processor is required by Union or Swedish law to process or disclose personal data, inform the customer before processing unless that law prohibits it; the processor does not disclose data voluntarily;

- k. not process special categories of personal data (Article 9) on the customer's behalf unless expressly agreed; the processor's staff work from Sweden and remote access to customer environments takes place only from the EU/EEA;
- l. where the processor administers the customer's Microsoft tenant, do so through delegated administration (Microsoft CSP/GDAP) with the permissions the customer has granted, which the customer may revoke at any time.

Assistance under d) and e) is included to a reasonable extent. Assistance beyond that is charged at the current hourly rate, agreed in advance.

5. Sub-processors

The customer gives general authorisation for the processor to engage sub-processors. The current list is in Annex 2 and at poise.se/en/trust. The processor notifies customers with an agreement at least 30 days before a new sub-processor is engaged. The customer may object within that period, and if no solution is reached the customer may terminate the affected service without charge. The processor contracts with each sub-processor on terms providing equivalent protection and remains liable to the customer for the sub-processor's processing.

6. Security measures

The processor maintains at least the following measures for its own infrastructure:

- encryption in transit (TLS 1.2 or later) and of stored secrets and backups;
- role-based permissions, personal accounts and multi-factor sign-in for all administration;
- continuous patching and hardening, network segmentation and firewalls;
- logging of administrative events;
- daily encrypted backups, both locally in the data centre and as an off-site copy at Wasabi in an EU region, with regularly tested restores;
- regular review of its own security with the same checks offered to customers.

Measures for platforms the customer licenses itself (Microsoft 365, Azure, Bitwarden) are set out in the respective provider's documentation.

7. Transfers to third countries

The processor's own processing takes place within the EU/EEA. Where a sub-processor has a parent company outside the EU/EEA, an EU region is used for storage and the EU–US Data Privacy Framework or the European Commission's standard contractual clauses serve as the transfer mechanism, per Annex 2. The processor does not otherwise transfer personal data to third countries without the customer's documented instruction.

8. Audits

The customer may, at most once a year or after an incident, audit the processor's compliance with this agreement. Audits take place with reasonable notice, during office hours and without disrupting operations, primarily by the processor providing documentation and answering questions. Costs of audits beyond this are borne by the customer.

9. Return and deletion

At the end of the service the processor, at the customer's choice, returns the personal data held in the processor's own infrastructure (hosting, servers, backups, ticketing) in a common format or deletes it, within 30 days, and confirms deletion in writing. Backups are deleted in the normal rotation, at the latest within 90 days. For platforms the customer licenses itself (for example Microsoft 365 and Bitwarden) the processor hands over the administrator role and removes its own permissions; the data remains with the customer. Data the processor must retain by law is excepted.

10. Liability

Each party's liability under this agreement follows the limitation of liability in the service agreement. Where the service agreement contains no limitation, each party's total liability under this agreement is limited to the fees the customer paid for the affected service in the twelve months preceding the event giving rise to liability. Administrative fines imposed by a supervisory authority are borne by the party on which they are imposed. The limitation does not apply in cases of intent or gross negligence.

11. Term and changes

This agreement applies for as long as the processor processes personal data on the customer's behalf. The processor may publish a new version; for existing customers the new version applies 30 days after notification. If the customer objects within that period, the previous version continues to apply to that customer until the parties agree, at the latest until the next renewal of the service agreement.

12. Governing law

Swedish law and the GDPR. Disputes are settled as set out in the service agreement.

Annex 1 – Processing details per service

SERVICE	SUBJECT MATTER AND NATURE	TYPES OF DATA	DATA SUBJECTS
Secure Workplace	Set-up and management of Microsoft 365, endpoint protection, password management, support, monthly report	Account and sign-in data, device data, security events, ticket history; temporary access to email and files during support	The customer's employees and contractors
Managed Security	As above plus protected network and Wi-Fi, network and security checks, security reviews	Network logs (IP addresses, device names), as above	As above plus visitors on the customer's network
Total IT	As above plus operation of servers, hosting, virtual machines, backups and licences	All content on servers and in backups, including email, files and databases	As above plus the customer's own customers and contacts in hosted systems
Add-on: Threat detection in Microsoft 365	Automated checks of sign-ins, rules, permissions and administrator accounts	Technical logs from Microsoft 365 (sign-in events, rule changes, app registrations)	The customer's employees

Add-on: Extended network analysis	Analysis of network traffic for anomalies	Traffic metadata, IP addresses, device identities	As Managed Security
Specialist engagements	Per the engagement description	Per the engagement description	Per the engagement description

Duration: the term of the service agreement.

Annex 2 – Sub-processors

Only suppliers that process personal data on the processor's behalf. Platforms the customer licenses itself (Microsoft 365, Azure, Bitwarden) are not sub-processors; there the customer is the contracting party and the processor the administrator.

SUB-PROCESSOR	SERVICE	REGION	TRANSFER MECHANISM
WatchGuard Technologies (US parent)	Firewall, Wi-Fi, AuthPoint MFA, FireCloud zero-trust remote access (point of presence in Stockholm)	EU	EU–US Data Privacy Framework / standard contractual clauses
Bitdefender (EU)	Protection of computers and servers (GravityZone)	EU	No transfer
Lettermint (EU)	Outbound email from the website and the services	EU	No transfer
Wasabi Technologies (US parent)	Encrypted off-site backups	EU	EU–US Data Privacy Framework / standard contractual clauses; copies are encrypted before they leave the processor
Bahnhof AB (Sweden)	Data centre and colocation for the processor's own servers; no logical access to data	Sweden	No transfer

The published list at poise.se/en/trust shows the same suppliers plus the customer's own platforms, marked by role.