Privacy Policy

Version 5 · updated: 03.10.2026

1. Data Controller

The controller of personal data processed in connection with the ESSW service and the operation of the customer portal admin.essw.pl is **AbejaIT Sp. z o.o.** with its registered office in Poznań, Aleja Wielkopolska 29 lok. 6, 60-603 Poznań, Poland, entered in the register of entrepreneurs of the Polish National Court Register (KRS) under number 0001235099 (District Court Poznań – Nowe Miasto i Wilda in Poznań, 8th Commercial Division of the KRS), tax ID (NIP): 7812108949; contact: e-mail biuro@abejait.pl (office) and awarie@abejait.pl (support/emergencies), phone +48 501 018 181 (sales), +48 512 222 240 (support/emergencies) (the “Controller”).

2. What Data We Process

- **Customer account and company data** — company name, tax ID (NIP), address, e-mail address, phone number, data of representatives and — to the extent required for certain documents — the PESEL number of a sole trader.
- **Customer portal user data** — name and surname, e-mail address, phone number, password (stored encrypted/hashed), two-factor authentication (2FA) settings.
- **Billing data** — history of orders, payments, invoices and accounting documents (including identifiers assigned by the payment operator and KSeF status).
- **Communication data** — content of support tickets, portal messenger messages, e-mail correspondence.
- **Technical data** — IP address, system logs, session identifiers, browser information; ERP instance health data (heartbeat, server resource metrics) to the extent not containing personal data of end contractors.

Data inside Customers’ ERP instances (e.g. data of contractors, suppliers of materials, purchase documents) is processed by us solely as a processor — on behalf of the Customer, who is its controller. Details are provided in the “GDPR — Data Processing Information” document.

3. Purposes and Legal Bases

Purpose	Legal basis (GDPR)
Conclusion and performance of the service agreement (account management, launching and maintaining the instance, support)	Art. 6(1)(b)
Billing, invoicing, tax and accounting obligations (including KSeF)	Art. 6(1)(c)
Electronic payment processing	Art. 6(1)(b) and (f)
Service security (logs, monitoring, backups, 2FA)	Art. 6(1)(f) — legitimate interest
Establishment, pursuit and defence of claims	Art. 6(1)(f)
Service-related communication (payment notices, maintenance, changes to terms)	Art. 6(1)(b) and (f)

4. Data Recipients

Data may be entrusted to or shared with the following categories of recipients — only to the extent necessary to provide the service:

- server infrastructure providers (hosting of instances and the portal),
- the external backup storage provider (backups are encrypted before transfer),
- the electronic payment operator (transaction processing),
- e-mail and SMS delivery providers (notifications),
- DNS/CDN service providers,
- the Polish National e-Invoicing System (KSeF) — with respect to invoice data, as required by law,
- entities providing accounting or legal services to the Controller,
- public authorities, where required by law.

5. Data Processing Location and Sub-processors (EU/EEA)

Data processed in connection with the Service — ERP instances, backups and network traffic — is stored and processed **within the European Union / European Economic Area (EU/EEA)**. The Controller uses the following trusted sub-processors, selecting their EU/EEA-located regions/data centres:

Sub-processor	Role	Data location	Privacy information
Hetzner Online GmbH	Server infrastructure (hosting of ERP instances and the portal)	Data centres in Germany and Finland (EU/EEA)	hetzner.com/legal/privacy-policy
Backblaze (EU region)	External, encrypted backup storage	EU region (data centre in Amsterdam, the Netherlands)	backblaze.com/company/privacy
Amazon Web Services (AWS), EU region	Infrastructure/storage (optional, EU regions, e.g. Frankfurt/Ireland)	EU/EEA regions	aws.amazon.com/compliance/gdpr-center
Cloudflare, Inc.	DNS/CDN services and attack protection	Processing with an EU data localization option	cloudflare.com/trust-hub/gdpr

A data processing agreement (DPA) compliant with Art. 28 GDPR is in place with each sub-processor. Backups are additionally encrypted (AES-256) with a key not available to the storage provider. Should, in exceptional cases, any data transfer take place outside the EEA, it occurs solely on the basis of mechanisms provided for in the GDPR (including standard contractual clauses — SCCs), with appropriate safeguards.

6. Retention Periods

- account and agreement data — for the duration of the agreement and afterwards until the expiry of the limitation period for claims;
- billing data and invoices — for the period required by tax law (as a rule, 5 years from the end of the tax year);
- ERP instance data and its backups — up to 30 days after termination of the agreement, after which they are permanently deleted;
- technical logs — up to 12 months;
- correspondence and tickets — up to 3 years after the matter is closed.

7. Data Subject Rights

Every person has the right to: access their data, rectify it, erase it, restrict processing, data portability, object to processing based on legitimate interest, and lodge a complaint with the President of the Personal Data Protection Office (uodo.gov.pl). Requests may be sent to biuro@abejait.pl.

8. Voluntary Provision of Data

Providing data is voluntary but necessary to conclude and perform the agreement and to issue billing documents. Without it, the service cannot be provided.

9. Automated Decision-Making

The Controller does not make decisions based solely on automated processing, including profiling, that would produce legal effects. System automations (e.g. suspension of an instance after the grace period for non-payment) follow directly from the terms of the agreement and can be reviewed by an operator at the Customer’s request.

10. Security

We apply technical and organisational measures adequate to the risk, including: encryption in transit (TLS), encrypted backups, two-factor authentication for operators and portal users, separation of Customer instances, availability monitoring and regular software updates.

11. “zlom.io KasaIntegrator” browser extension

The zlom.io KasaIntegrator extension (Chrome / Edge), published by AbejaIT Sp. z o.o., connects your company's system with a fiscal printer on the company's local network. It passes commands prepared by the system (e.g. a receipt, a daily report, a non-fiscal printout) to the printer and returns the result to the system.

- **Connections:** only the two addresses entered in the extension settings — your company's system instance server (HTTPS) and the fiscal printer on the local network (LAN). The extension does not connect to the Operator, to Google or to any other party.
- **Stored in the browser:** three settings (system address, printer IP address and port — entered by the user or pre-filled by the IT department through a company policy), a device key (the private key never leaves the extension storage and cannot be exported) and a log of the command in progress, deleted when the command is finished.
- **Transferred:** command content (e.g. receipt items, amounts and payment method) only between the system instance server and the printer; to the system instance server — the device public key, the extension version and the browser and operating system name as a workstation description.
- **Not done:** the extension does not collect personal data (receipts with a buyer's tax ID are rejected), does not read other websites, does not collect browsing history, uses no analytics or ads and does not share data with third parties.
- **Deletion:** uninstalling the extension removes its settings, key and log from the browser. The workstation can also be disconnected in the system (“Workstations” list).

12. Changes to this Policy

This Policy may be updated as the service evolves. The current version is always available in the Customer Portal; we notify about material changes via the portal or e-mail.