



Polityka prywatności

Wersja 4 · aktualizacja: 15.07.2026

1. Administrator danych

Administratorem danych osobowych przetwarzanych w związku ze świadczeniem usługi ESSW oraz działaniem portalu klienta admin.essw.pl jest **AbejaIT Sp. z o.o.** z siedzibą w Poznaniu, Aleja Wielkopolska 29 lok. 6, 60-603 Poznań, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 0001235099 (Sąd Rejonowy Poznań – Nowe Miasto i Wilda w Poznaniu, VIII Wydział Gospodarczy KRS), NIP 7812108949; kontakt: e-mail biuro@abejait.pl (biuro) i awarie@abejait.pl (wsparcie/awarie), tel. +48 501 018 181 (sprzedaż), +48 512 222 240 (wsparcie/awarie) (dalej: „Administrator”).

2. Jakie dane przetwarzamy

- **Dane konta i firmy Klienta** — nazwa firmy, NIP, adres, adres e-mail, numer telefonu, dane osób reprezentujących oraz — w zakresie wymaganym do wystawienia niektórych dokumentów — PESEL osoby fizycznej prowadzącej działalność.
- **Dane użytkowników portalu klienta** — imię i nazwisko, adres e-mail, numer telefonu, hasło (w postaci zaszyfrowanej), ustawienia dwuskładnikowego uwierzytelniania (2FA).
- **Dane rozliczeniowe** — historia zamówień, płatności, faktur i dokumentów księgowych (w tym identyfikatory nadane przez operatora płatności i status w KSeF).
- **Dane komunikacji** — treść zgłoszeń wsparcia, wiadomości w komunikatorze portalu, korespondencja e-mail.
- **Dane techniczne** — adres IP, logi systemowe, identyfikatory sesji, informacje o przeglądarce; dane o stanie instancji ERP (heartbeat, metryki zasobów serwera) w zakresie niezawierającym danych osobowych końcowych kontrahentów.

Dane w instancjach ERP Klientów (np. dane kontrahentów, dostawców surowców, dokumenty skupu) przetwarzamy wyłącznie jako podmiot przetwarzający — na zlecenie Klienta, który jest ich administratorem. Szczegóły w dokumencie „RODO — informacje”.

3. Cele i podstawy prawne przetwarzania

Cel	Podstawa prawna (RODO)
Zawarcie i wykonanie umowy o świadczenie usługi (prowadzenie konta, uruchomienie i utrzymanie instancji, wsparcie)	art. 6 ust. 1 lit. b
Rozliczenia, wystawianie faktur, obowiązki podatkowe i księgowe (w tym KSeF)	art. 6 ust. 1 lit. c
Obsługa płatności elektronicznych	art. 6 ust. 1 lit. b i f
Zapewnienie bezpieczeństwa usługi (logi, monitoring, kopie zapasowe, 2FA)	art. 6 ust. 1 lit. f — prawnie uzasadniony interes
Ustalenie, dochodzenie i obrona roszczeń	art. 6 ust. 1 lit. f
Komunikacja w sprawach usługi (powiadomienia o płatnościach, pracach technicznych, zmianach regulaminu)	art. 6 ust. 1 lit. b i f

4. Odbiorcy danych

Dane mogą być powierzane lub udostępniane następującym kategoriom odbiorców — wyłącznie w zakresie niezbędnym do świadczenia usługi:

- dostawcy infrastruktury serwerowej (hosting instancji i portalu),
- dostawcy zewnętrznego magazynu kopii zapasowych (kopie są szyfrowane przed przekazaniem),
- operatorowi płatności elektronicznych (w zakresie obsługi transakcji),
- dostawcy usług wysyłki e-mail i SMS (powiadomienia),
- dostawcy usług DNS/CDN,
- Krajowemu Systemowi e-Faktur (KSeF) — w zakresie danych faktur, zgodnie z przepisami,
- podmiotom świadczącym obsługę księgową lub prawną Administratora,
- organom publicznym, gdy obowiązek taki wynika z przepisów prawa.

5. Lokalizacja przetwarzania danych i podprocesorzy (UE/EOG)

Dane przetwarzane w związku z Usługą — instancje ERP, kopie zapasowe oraz ruch sieciowy — są przechowywane i przetwarzane **na terenie Unii Europejskiej / Europejskiego Obszaru Gospodarczego (UE/EOG)**. Administrator korzysta z następujących zaufanych podprocesorów, wybierając ich regiony/centra danych zlokalizowane w UE/EOG:

Podprocesor	Rola	Lokalizacja danych	Informacja o prywatności
Hetzner Online GmbH	Infrastruktura serwerowa (hosting instancji ERP i portalu)	Centra danych w Niemczech i Finlandii (UE/EOG)	hetzner.com/legal/privacy-policy
Backblaze (region UE)	Zewnętrzny, zaszyfrowany magazyn kopii zapasowych	Region UE (centrum danych w Amsterdamie, Holandia)	backblaze.com/company/privacy
Amazon Web Services (AWS), region UE	Infrastruktura/magazyn (opcjonalnie, regiony UE, np. Frankfurt/Irlandia)	Regiony UE/EOG	aws.amazon.com/compliance/gdpr-center
Cloudflare, Inc.	Usługi DNS/CDN i ochrona przed atakami	Przetwarzanie z opcją lokalizacji w UE (EU Data Localization)	cloudflare.com/trust-hub/gdpr

Z każdym podprocesorem zawarto umowę powierzenia przetwarzania (DPA) zgodną z art. 28 RODO. Kopie zapasowe są dodatkowo szyfrowane (AES-256) kluczem, którym nie dysponuje dostawca magazynu. Jeżeli w wyjątkowych sytuacjach jakiegokolwiek transfer danych miałby nastąpić poza EOG, odbywa się on wyłącznie na podstawie mechanizmów przewidzianych w RODO (m.in. standardowych klauzul umownych — SCC), z zachowaniem odpowiednich zabezpieczeń.

6. Okres przechowywania

- dane konta i umowy — przez czas trwania umowy, a po jej zakończeniu do upływu okresu przedawnienia roszczeń;
- dane rozliczeniowe i faktury — przez okres wymagany przepisami podatkowymi (co do zasady 5 lat od końca roku podatkowego);
- dane instancji ERP i jej kopie zapasowe — do 30 dni po zakończeniu umowy, po czym są trwale usuwane;
- logi techniczne — do 12 miesięcy;
- korespondencja i zgłoszenia — do 3 lat od zakończenia sprawy.

7. Prawa osób, których dane dotyczą

Każdej osobie przysługuje prawo: dostępu do danych, sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych, sprzeciwu wobec przetwarzania opartego na prawnie uzasadnionym interesie oraz wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (uodo.gov.pl). Wnioski można kierować na adres biuro@abejait.pl.

8. Dobrowolność podania danych

Podanie danych jest dobrowolne, ale niezbędne do zawarcia i wykonania umowy oraz wystawienia dokumentów rozliczeniowych. Bez ich podania świadczenie usługi nie jest możliwe.

9. Zautomatyzowane podejmowanie decyzji

Administrator nie podejmuje wobec osób decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, które wywoływałyby skutki prawne. Automatyzacje systemowe (np. zawieszenie instancji po upływie okresu karencji za brak płatności) wynikają wprost z warunków umowy i mogą zostać zweryfikowane przez operatora na wniosek Klienta.

10. Bezpieczeństwo

Stosujemy środki techniczne i organizacyjne adekwatne do ryzyka, w tym: szyfrowanie transmisji (TLS), szyfrowanie kopii zapasowych, dwuskładnikowe uwierzytelnianie operatorów i użytkowników portalu, separację instancji Klientów, monitoring dostępności oraz regularne aktualizacje oprogramowania.

11. Zmiany polityki

Polityka może być aktualizowana wraz z rozwojem usługi. Aktualna wersja jest zawsze dostępna w Portalu Klienta; o istotnych zmianach informujemy przez portal lub e-mail.