

ZAŁĄCZNIK NR 1 DO REGULAMINU – UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

§1. Strony i zawarcie Umowy

1. **Administrator / Podmiot powierzający** – Klient (biuro rachunkowe) w rozumieniu Regulaminu.
2. **Podmiot przetwarzający** – **BL SOFT sp. z o.o.**, dane jak w §1 Regulaminu (dalej: **Procesor**).
3. Umowa zostaje zawarta z chwilą akceptacji Regulaminu i utworzenia Konta, na czas obowiązywania Umowy głównej. Regulamin wraz z niniejszym Załącznikiem stanowi inny instrument prawny w rozumieniu art. 28 ust. 3 RODO; Procesor utrzuła datę, wersję dokumentów i konto, z którego dokonano akceptacji, i przekazuje Klientowi ich treść na trwałym nośniku.
4. **Łańcuch powierzenia.** Klient oświadcza, że jest administratorem danych albo podmiotem przetwarzającym dane Klientów Końcowych. Jeżeli Klient jest podmiotem przetwarzającym, oświadcza, że **posiada zgodę administratora na dalsze powierzenie** przetwarzania (art. 28 ust. 2 i 4 RODO), a niniejsza Umowa stanowi wówczas umowę dalszego powierzenia, w której Procesor występuje jako dalszy podmiot przetwarzający.

§2. Przedmiot, charakter i cel przetwarzania

1. **Cel:** wykonywanie Usługi opisanej w §3 Regulaminu – monitorowanie kompletności dokumentów księgowych Klientów Końcowych, weryfikacja kontrahentów w wykazie podatników VAT, zestawianie płatności i generowanie raportów oraz przypomnień.
2. **Charakter przetwarzania:** zbieranie (pobieranie z KSeF i z plików wgrywanych przez Klienta), przechowywanie, porządkowanie, zestawianie, analizowanie, udostępnianie Klientowi, usuwanie.
3. **Czas przetwarzania:** przez czas obowiązywania Umowy głównej oraz przez okresy wskazane w §8.

§3. Rodzaj danych i kategorie osób

1. **Kategorie osób, których dane dotyczą:**
 - a) osoby prowadzące jednoosobową działalność gospodarczą będące Klientami Końcowymi Klienta,
 - b) kontrahenci (sprzedawcy i nabywcy) występujący na fakturach Klientów Końcowych – w tym osoby fizyczne prowadzące działalność gospodarczą,
 - c) osoby fizyczne nieprowadzące działalności, jeżeli występują jako nabywcy na fakturach Klientów Końcowych przesłanych do KSeF – Usługa **nie zapisuje ich danych identyfikujących** (ani nazwy, ani adresu); z takiej faktury pozostają wyłącznie numer, daty, kwoty i waluta,
 - d) osoby reprezentujące lub kontaktowe wskazane przez Klienta.
2. **Rodzaj danych:**
 - a) dane identyfikacyjne i kontaktowe Klientów Końcowych: nazwa/firma, NIP, adres e-mail do korespondencji, kwota abonamentu księgowego ustalona z Klientem (wraz z historią jej zmian: od którego miesiąca obowiązuje dana kwota), znacznik rezygnacji z przypomnień oraz ustawienia kontroli (próg duplikatów, termin płatności, potwierdzenie, że wgrane wyciągi bankowe obejmują wszystkie rachunki Klienta Końcowego, przełącznik podpowiedzi AI z lit. c) – Usługa **nie przechowuje adresów pocztowych**;
 - b) dane z **nagłówków faktur** pobranych z KSeF: numer faktury, daty, kierunek (sprzedaż/zakup), identyfikator kontrahenta (NIP albo numer VAT-UE – **bez nazwy i adresu**), kwoty netto/VAT/brutto, waluta, numer referencyjny KSeF;
faktur zakupowych i sprzedażowych powyżej 15 000 zł, przedstawionych między przedsiębiorcami dodatkowo: oznaczenie mechanizmu podzielonej płatności, **numery rachunków bankowych sprzedawcy** wskazane na fakturze (faktury zakupowe) oraz **pozycje faktury** – nazwa towaru lub usługi, wartość netto, stawka VAT i kody wpisane przez wystawcę (PKWiU, CN, GTU, znacznik załącznika nr 15 do ustawy o VAT) – pobierane z pełnej treści faktury wyłącznie w tym zakresie, wraz z automatyczną oceną obowiązku MPP wyprowadzoną z tych kodów oraz – wyłącznie po włączeniu tej opcji przez Klienta dla wszystkich albo

wybranych Klientów Końcowych (domyślnie jest wyłączona) – z podpowiedzi modelu językowego, któremu Procesor przekazuje same nazwy pozycji faktury (bez kwot, numeru faktury, numerów NIP i nazw stron), a także decyzją Klienta („podlega / nie podlega”), jej datą, notatką i oznaczeniem Użytkownika, który ją zapisał;

d) dane z wyciągów bankowych w formacie MT940 wgranych przez Klienta: kwoty, daty, tytuły i strony operacji;

e) wpisy dziennika zdarzeń Klienta (kto z Użytkowników Klienta i kiedy wykonał operację na danych Klientów Końcowych); dane kont Użytkowników (adres e-mail, rola, uprawnienia, dane uwierzytelniające) Procesor przetwarza jako administrator, na zasadach określonych w Polityce prywatności;

Poświadczenie KSeF Klienta (certyfikat z kluczem prywatnym) albo token) – przechowywane w postaci zaszyfrowanej;

g) wyniki sprawdzeń w publicznym wykazie podatników VAT – status i nazwa podmiotu dla NIP oraz odpowiedź wykazu, czy numer rachunku z faktury zakupowej figuruje przy danym NIP (NIP, numer rachunku, odpowiedź, identyfikator zapytania, data) – pamięć podręczna wspólna dla wszystkich Klientów (jawne dane rejestrowe, odtwarzalne z wykazu w każdej chwili); zapis, że dany Klient sprawdził dany NIP (Klient, NIP, czas sprawdzenia, dzień, na który wykaz podał status, czas zapytania do wykazu, identyfikator zapytania wykazu), jest prowadzony osobno dla każdego Klienta i usuwany razem z jego kontem.

3. Procesor **nie przetwarza szczególnych kategorii danych** (art. 9 RODO) ani danych dotyczących wyroków skazujących (art. 10 RODO); Klient zobowiązuje się nie wprowadzać takich danych do Usługi **ani nie przekazywać ich Procesorowi w korespondencji, w tym pocztą elektroniczną** (Regulamin §11 ust. 4).

§4. Obowiązki Procesora

Procesor zobowiązuje się do:

1. przetwarzania danych **wyłącznie na udokumentowane polecenie** Klienta; za takie polecenie uznaje się zawarcie niniejszej Umowy oraz czynności podejmowane przez Użytkowników w panelu Usługi. Dotyczy to także ewentualnego przekazywania danych do państwa trzeciego – Procesor nie przekazuje danych poza EOG (§7). Wyjątkiem jest obowiązek nałożony na Procesora przez prawo Unii lub prawo polskie – wówczas Procesor informuje Klienta o tym obowiązku przed rozpoczęciem przetwarzania, chyba że prawo zabrania udzielenia takiej informacji z uwagi na ważny interes publiczny;
2. zapewnienia, by osoby upoważnione do przetwarzania danych **zobowiązały się do zachowania tajemnicy** lub podlegały ustawowemu obowiązkowi tajemnicy;
3. stosowania środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania (art. 32 RODO) – wykaz w §9;
4. przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego (§6);
5. **pomocy Klientowi** – w miarę możliwości i za pomocą odpowiednich środków technicznych – w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą (rozdział III RODO);
6. **pomocy Klientowi** w wywiązywaniu się z obowiązków określonych w art. 32–36 RODO (bezpieczeństwo, zgłaszanie naruszeń, ocena skutków dla ochrony danych), uwzględniając charakter przetwarzania i dostępne Procesorowi informacje; w tym celu Procesor udostępnia Klientowi opis operacji przetwarzania, kategorii danych, odbiorców, okresów przechowywania i środków bezpieczeństwa w postaci umożliwiającej wykorzystanie w ocenie skutków dla ochrony danych (art. 35 ust. 7 RODO);
7. **usunięcia lub zwrotu** danych po zakończeniu świadczenia usług – zgodnie z §8;
8. udostępniania Klientowi informacji niezbędnych do wykazania spełnienia obowiązków z art. 28 RODO oraz umożliwienia audytów – zgodnie z §10;
9. **niezwłocznego informowania Klienta**, jeżeli w ocenie Procesora wydane polecenie stanowi naruszenie RODO lub innych przepisów o ochronie danych.

§5. Obowiązki Klienta

1. Klient oświadcza, że dysponuje podstawą prawną do przetwarzania danych powierzonych Procesorowi oraz do ich powierzenia.

2. Klient wprowadza do Usługi wyłącznie dane niezbędne do jej wykonywania i zobowiązuje się nie przekazywać danych wskazanych w §3 ust. 3.
3. Klient zarządza uprawnieniami swoich Użytkowników w panelu Usługi i odpowiada za ich aktualność (odbieranie dostępu byłym pracownikom).
4. Klient odpowiada za nadanie i utrzymanie uprawnień w KSeF oraz za ważność Poświadczenia KSeF.

§6. Podpowierzenie (dalsi przetwarzający)

1. Klient udziela Procesorowi **ogólnej zgody** na korzystanie z usług dalszych podmiotów przetwarzających, wskazanych w **Załączniku nr 2** do Regulaminu (lista podwykonawców, publikowana na stronie fakturoskop.pl). 1a. Procesor korzysta wyłącznie z dalszych podmiotów przetwarzających, które przetwarzają dane na terenie Europejskiego Obszaru Gospodarczego, zawarły z Procesorem umowę powierzenia zgodną z art. 28 RODO, stosują szyfrowanie danych w spoczynku i w transmisji oraz udostępniają dokumentację środków bezpieczeństwa.
2. Procesor nakłada na dalsze podmioty przetwarzające **te same obowiązki ochrony danych**, jakie wynikają z niniejszej Umowy, i **odpowiada wobec Klienta za ich działania i zaniechania** jak za własne (art. 28 ust. 4 RODO).
3. O zamierzonej zmianie listy (dodaniu lub zastąpieniu podwykonawcy) Procesor informuje Klienta **e-mailem oraz w Usłudze z co najmniej 14-dniowym wyprzedzeniem**.
4. Klient może wnieść **umotywowany sprzeciw w terminie 14 dni** od otrzymania informacji. W razie sprzeciwu Strony podejmują rozmowy w celu znalezienia rozwiązania; jeżeli nie jest ono możliwe, Klient może wypowiedzieć Umowę główną ze skutkiem na dzień planowanej zmiany, a Procesor zwraca opłatę za niewykorzystany okres.

§7. Lokalizacja przetwarzania i transfery poza EOG

1. Dane są przetwarzane **na terenie Europejskiego Obszaru Gospodarczego**; serwery aplikacji i baza danych znajdują się w Polsce (Warszawa). Jedyna operacja poza Polską to — wyłącznie po włączeniu tej opcji przez Klienta, dla wszystkich albo wybranych Klientów Końcowych (domyślnie wyłączonej) — odpowiedź modelu językowego dla nazw pozycji faktur powyżej 15 000 zł, wykonywana u podwykonawcy wskazanego w Załączniku nr 2 we Francji (Paryż), bez przechowywania treści zapytań przez tego podwykonawcę.
2. Procesor **nie przekazuje danych osobowych do państw trzecich**. Kanał powiadomień technicznych operatora (ntfy) przenosi wyłącznie metadane techniczne (nazwa usługi, kod błędu, adres bez parametrów, identyfikator żądania i biura, NIP-y maskowane) — bez danych osobowych Klientów Końcowych.
3. Gdyby przekazanie poza EOG stało się niezbędne, Procesor poinformuje Klienta z wyprzedzeniem i zapewni podstawę z rozdziału V RODO; Klientowi przysługuje wówczas prawo sprzeciwu i wypowiedzenia na zasadach z §6 ust. 4.

§8. Zwrot i usunięcie danych

1. Po rozwiązaniu Umowy głównej Klient ma **30 dni** na złożenie wniosku o zwrot danych; Procesor przekazuje wówczas eksport w powszechnie używanym formacie (CSV) i usuwa dane po jego przekazaniu, nie później niż w terminie z ust. 2.
2. Jeżeli Klient nie złoży wniosku, po upływie tego terminu Procesor **trwale usuwa** dane Klienta z systemów produkcyjnych wraz z istniejącymi kopiami (art. 28 ust. 3 lit. g RODO). Z kopii zapasowych dane znikają wraz z ich rotacją, najpóźniej w ciągu kolejnych **14 dni**.
3. Procesor może zachować dane wyłącznie w zakresie i przez okres wymagany przepisami prawa — dokumentację rozliczeniową Umowy głównej (dane identyfikacyjne Klienta, historia abonamentu, faktury za Usługę) oraz dowód zawarcia Umowy (data i wersja zaakceptowanych dokumentów, adres e-mail Konta i adres IP, z którego dokonano akceptacji, złożone oświadczenia) przez **5 lat od końca roku podatkowego** — informując o tym Klienta przy usunięciu pozostałych danych.
4. Na wniosek Klienta Procesor potwierdza usunięcie danych na piśmie lub e-mailem.

§9. Środki techniczne i organizacyjne (art. 32 RODO)

1. Procesor stosuje w szczególności:
 - a) **szyfrowanie sekretów** — Poświadczenia KSeF i sekrety 2FA szyfrowane AES-256-GCM, klucz przechowywany poza bazą danych; rotacja klucza obsługiwana proceduralnie; hasła Użytkowników przechowywane wyłącznie jako skrót (argon2);
 - szyfrowanie w spoczynku** — baza danych z szyfrowaniem at-rest; kopie zapasowe szyfrowane (age) w chwili powstania, nigdy nie zapisywane w postaci jawnej;
 - szyfrowanie transmisji** — TLS dla ruchu użytkowników oraz TLS z pełną weryfikacją certyfikatu (verify-full) dla połączeń z bazą;
 - d) **kontrolę dostępu** — obowiązkowe uwierzytelnianie dwuetapowe (TOTP) dla wszystkich Użytkowników, blokada konta na 15 minut po 5 nieudanych próbach, role uprawnień, sesja wygasająca po 24 godzinach od ostatniej aktywności i najpóźniej 7 dni od zalogowania, zapamiętanie zaufanego urządzenia najwyżej na 30 dni (odwoływalne przez Użytkownika);
 - izolację danych między Klientami** wymuszającą na dwóch poziomach — w każdym zapytaniu aplikacji oraz w samej bazie danych (polityki wierszowe, Row Level Security, których połączenie aplikacji nie może ominąć) — objętą automatycznymi testami regresyjnymi;
 - rozliczalność** — dziennik zdarzeń (audyt) dostępny dla Klienta w panelu Usługi, przechowywany 24 miesiące;
 - minimalizację w logach** — maskowanie numerów NIP; telemetria błędów ograniczona listą dozwolonych pól (bez treści żądań i nagłówek), przechowywana 30 dni, bez kopii zapasowych;
 - kopie zapasowe** — codzienne, szyfrowane w chwili powstania, z kopią u drugiego dostawcy (Warszawa) chronioną przed usunięciem i modyfikacją przez 13 dni (blokada obiektów), retencja 14 dni, test odtworzenia co kwartał wg kalendarza przeglądów;
 - monitoring i alerty bezpieczeństwa** — automatyczne powiadomienia o zdarzeniach istotnych dla bezpieczeństwa (m.in. logowania do panelu operatora, blokady kont, dostęp administracyjny do serwerów);
 - proces wytwarzania** — testy automatyczne, przegląd bezpieczeństwa zmian przed wydaniem, skanowanie zależności pod kątem podatności, skanowanie repozytorium pod kątem sekretów;
 - ograniczenie ruchu wychodzącego** — składniki Usługi na serwerze mogą łączyć się wyłącznie z listą znanych adresów (KSeF, wykaz podatników VAT, NBP, serwer poczty, własny system alertów, model językowy po włączeniu przez Klienta, urząd certyfikacji); każda inna próba połączenia jest odrzucana na zaporze serwera i zgłaszana jako alert bezpieczeństwa.
2. Aktualny, szczegółowy opis środków Procesor udostępnia na żądanie Klienta (dokument „Bezpieczeństwo Fakturoskopu”).
3. Procesor może zmieniać środki, pod warunkiem że poziom ochrony nie ulegnie obniżeniu.

§10. Naruszenia ochrony danych

1. Procesor **bez zbędnej zwłoki** po stwierdzeniu naruszenia ochrony danych osobowych zgłasza je Klientowi na adres e-mail wskazany w panelu Usługi.
2. Zgłoszenie zawiera — w miarę dostępnych informacji — opis charakteru naruszenia, kategorie i przybliżoną liczbę osób i wpisów, możliwe konsekwencje oraz zastosowane lub proponowane środki zaradcze.
3. Obowiązek zgłoszenia naruszenia organowi nadzorcemu (art. 33 ust. 1 RODO) oraz zawiadomienia osób (art. 34 RODO) spoczywa na Kliencie jako administratorze; Procesor udziela mu niezbędnej pomocy.

§11. Audyt i kontrola

1. Klient ma prawo do audytu przestrzegania niniejszej Umowy, nie częściej niż **raz w roku kalendarzowym** (oraz każdorazowo po stwierdzonym naruszeniu), po uprzedzeniu Procesora z co najmniej **7-dniowym** wyprzedzeniem.
2. Audyt odbywa się w godzinach pracy, w sposób nie zakłócający działalności Procesora, przez osoby zobowiązane do poufności; audyt nie może naruszać tajemnicy przedsiębiorstwa ani bezpieczeństwa danych innych klientów Procesora.

3. Koszty audytu ponosi Klient, w tym uzasadnione koszty zaangażowania Procesora, chyba że audyt wykaże istotne naruszenie niniejszej Umowy.
4. Procesor może wykazać zgodność, przedstawiając aktualną dokumentację środków bezpieczeństwa, wyniki testów lub raporty z przeglądów.

§12. Postanowienia końcowe

1. W sprawach nieuregulowanych stosuje się RODO, przepisy prawa polskiego oraz postanowienia Regulaminu.
2. Zmiana niniejszej Umowy następuje w trybie zmiany Regulaminu (§12 Regulaminu) i wymaga akceptacji zmienionej Umowy przez Klienta w Usłudze.
3. W razie sprzeczności między Regulaminem a niniejszą Umową – w zakresie ochrony danych osobowych pierwszeństwo ma niniejsza Umowa.