Umowa powierzenia przetwarzania danych osobowych — IT Excellence

Załącznik nr 2 do Regulaminu produktów i usług chmurowych IT Excellence oraz do Regulaminu świadczenia usługi eHandel365 · Wersja: wrzesień 2026 · Obowiązuje od: 23 września 2026

IT Excellence S.A. · ul. Kolejowa 15/17, 01-217 Warszawa · KRS 0001082807 · NIP 5214040057

Niniejsza Umowa powierzenia przetwarzania danych osobowych (**Umowa powierzenia**) określa zasady przetwarzania przez IT Excellence danych osobowych, których administratorem jest Klient, w związku ze świadczeniem Usługi. Umowa powierzenia jest zawierana na podstawie art. 28 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (**RODO**).

Akceptacja Regulaminu jest równoznaczna z zawarciem niniejszej Umowy powierzenia. Umowa powierzenia wchodzi w życie z dniem zawarcia Umowy i obowiązuje przez cały okres jej trwania.

Regulamin oznacza w niniejszym dokumencie Regulamin produktów i usług chmurowych IT Excellence albo Regulamin świadczenia usługi eHandel365 — ten z nich, który ma zastosowanie do Usługi zamówionej przez Klienta. Pozostałe pojęcia pisane wielką literą, a niezdefiniowane w Umowie powierzenia, mają znaczenie nadane im w Regulaminie.

Strony:

- **Administrator** — Klient, tj. podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych wprowadzanych do Usługi;
- **Podmiot przetwarzający** — IT Excellence spółka akcyjna z siedzibą w Warszawie, ul. Kolejowa 15/17, 01-217 Warszawa, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie pod numerem KRS 0001082807, NIP 5214040057, REGON 526561240.

Jeżeli Klient sam jest podmiotem przetwarzającym wobec danych, które wprowadza do Usługi (w szczególności gdy Klient jest Biurem rachunkowym przetwarzającym dane na zlecenie swoich klientów), niniejsza Umowa powierzenia stanowi dalsze powierzenie w rozumieniu art. 28 ust. 4 RODO. W takim przypadku Klient oświadcza, że posiada zgodę swojego administratora na dalsze powierzenie oraz że warunki niniejszej Umowy powierzenia są nie mniej rygorystyczne niż warunki umowy łączącej go z tym administratorem.

1. Przedmiot i charakter przetwarzania

1.1. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych w zakresie i w celach określonych w **Załączniku A** do Umowy powierzenia.

1.2. Przetwarzanie odbywa się wyłącznie w celu świadczenia Usługi zgodnie z Umową, w tym jej utrzymania, usuwania Usterek, zapewnienia bezpieczeństwa oraz wykonania obowiązków wynikających z przepisów prawa ciążących na Podmiocie przetwarzającym.

1.3. Podmiot przetwarzający nie ustala celów ani sposobów przetwarzania powierzonych danych. Zakres i rodzaj danych wprowadzanych do Usługi określa wyłącznie Administrator — przez konfigurację Instancji Klienta, definiowanie pól dodatkowych i modułów własnych oraz przez faktyczne działania Użytkowników.

1.4. Przetwarzanie ma charakter ciągły i trwa przez okres obowiązywania Umowy, z zastrzeżeniem Rozdziału 10.

2. Polecenia Administratora

2.1. Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora, w tym w zakresie przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej — chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

2.2. Za udokumentowane polecenie Administratora uznaje się: (a) zawarcie Umowy i akceptację Regulaminu, (b) korzystanie przez Administratora i Użytkowników z funkcjonalności Usługi zgodnie z jej przeznaczeniem, (c) konfigurację Instancji Klienta dokonaną przez Administratora, (d) zgłoszenia i dyspozycje przekazane Podmiotowi przetwarzającemu w formie dokumentowej przez osoby wskazane w Zamówieniu.

2.3. Podmiot przetwarzający niezwłocznie informuje Administratora, jeżeli jego zdaniem wydane polecenie stanowi naruszenie RODO lub innych przepisów o ochronie danych osobowych. Do czasu wyjaśnienia Podmiot przetwarzający może wstrzymać wykonanie takiego polecenia.

2.4. Wykonanie polecenia Administratora wykraczającego poza standardowe funkcjonalności Usługi (w szczególności nietypowy eksport, migracja, odtworzenie danych z kopii zapasowej na żądanie) może wymagać odrębnego uzgodnienia i zostać objęte dodatkowym wynagrodzeniem.

3. Obowiązki Podmiotu przetwarzającego

3.1. Podmiot przetwarzający zobowiązuje się:

1. przetwarzać dane osobowe wyłącznie w zakresie i celu określonym w Umowie powierzenia;
2. zapewnić, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
3. nadawać upoważnienia do przetwarzania danych osobowych wyłącznie osobom, którym dostęp do danych jest niezbędny, oraz prowadzić ewidencję tych upoważnień;
4. podjąć środki wymagane na mocy art. 32 RODO, opisane w **Załączniku B**;
5. przestrzegać warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w Rozdziale 4;
6. biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomagać Administratorowi — poprzez odpowiednie środki techniczne i organizacyjne — wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w Rozdziale III RODO;
7. pomagać Administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO, uwzględniając charakter przetwarzania oraz dostępne mu informacje;
8. po zakończeniu świadczenia Usługi usunąć lub zwrócić Administratorowi dane osobowe na zasadach określonych w Rozdziale 10;
9. udostępniać Administratorowi informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwiać audyty na zasadach określonych w Rozdziale 8;
10. prowadzić rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora, zgodnie z art. 30 ust. 2 RODO.

3.2. Podmiot przetwarzający nie wykorzystuje powierzonych danych osobowych do własnych celów, w szczególności do celów marketingowych, analitycznych ani do trenowania modeli uczenia maszynowego. Podmiot przetwarzający może wykorzystywać dane zagregowane i zanonimizowane — niepozwalające na identyfikację Administratora ani osób fizycznych — w celach statystycznych i rozwojowych.

4. Dalsze powierzenie (podprzetwarzający)

4.1. Administrator udziela Podmiotowi przetwarzającemu **ogólnej zgody** na korzystanie z usług innych podmiotów przetwarzających (**Podprzetwarzających**), w rozumieniu art. 28 ust. 2 zdanie pierwsze RODO.

4.2. Aktualny wykaz Podprzetwarzających stanowi **Załącznik C** i jest publikowany pod adresem https://ite.pl/podprzetwarzajacy.

4.3. Podmiot przetwarzający informuje Administratora o zamierzonych zmianach dotyczących dodania lub zastąpienia Podprzetwarzających z co najmniej **30-dniowym wyprzedzeniem**, wiadomością e-mail na adres wskazany w Zamówieniu albo komunikatem w Programie.

4.4. Administrator może wyrazić uzasadniony sprzeciw wobec zmiany, o której mowa w pkt 4.3, w terminie 14 dni od otrzymania informacji, w formie dokumentowej. Sprzeciw powinien wskazywać konkretne ryzyko dla ochrony danych osobowych. W razie sprzeciwu Strony podejmą w dobrej wierze rozmowy zmierzające do jego rozstrzygnięcia. Jeżeli w terminie 30 dni nie osiągną porozumienia, a Podmiot przetwarzający nie jest w stanie świadczyć Usługi bez udziału danego Podprzetwarzającego, Administratorowi przysługuje prawo wypowiedzenia Umowy ze skutkiem na dzień poprzedzający wejście zmiany w życie, z prawem do zwrotu Opłaty za niewykorzystany okres — co stanowi wyjątek od zasady braku zwrotu Opłat wyrażonej w Regulaminie.

4.5. Podmiot przetwarzający nakłada na każdego Podprzetwarzającego, w drodze umowy, te same obowiązki ochrony danych, które spoczywają na nim samym na mocy Umowy powierzenia. Jeżeli Podprzetwarzający nie wywiąże się ze swoich obowiązków w zakresie ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków tego Podprzetwarzającego spoczywa na Podmiocie przetwarzającym.

---

5. Prawa osób, których dane dotyczą

5.1. Podmiot przetwarzający udostępnia Administratorowi funkcjonalności Usługi umożliwiające samodzielną realizację żądań osób, których dane dotyczą — w szczególności dostęp do danych, ich sprostowanie, usunięcie, ograniczenie przetwarzania oraz eksport danych w ustrukturyzowanym formacie nadającym się do odczytu maszynowego.

5.2. Jeżeli osoba, której dane dotyczą, zwróci się z żądaniem bezpośrednio do Podmiotu przetwarzającego, Podmiot przetwarzający nie realizuje takiego żądania samodzielnie — przekazuje je Administratorowi niezwłocznie, nie później niż **w terminie 3 Dni roboczych**, i informuje osobę składającą żądanie o przekazaniu, nie ujawniając przy tym informacji objętych poufnością.

5.3. Jeżeli realizacja żądania wykracza poza funkcjonalności Usługi, Podmiot przetwarzający udziela Administratorowi pomocy technicznej w rozsądnym zakresie; pomoc wykraczająca poza standardowe Wsparcie techniczne może zostać objęta odrębnym wynagrodzeniem.

---

6. Naruszenia ochrony danych osobowych

6.1. Podmiot przetwarzający zgłasza Administratorowi każde naruszenie ochrony danych osobowych dotyczące powierzonych danych **niezwłocznie, nie później niż w terminie 24 godzin** od jego stwierdzenia, wiadomością e-mail na adres kontaktowy wskazany w Zamówieniu.

6.2. Zgłoszenie zawiera co najmniej: (a) opis charakteru naruszenia, w tym — w miarę możliwości — kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie; (b) imię, nazwisko i dane kontaktowe osoby, od której można uzyskać więcej informacji; (c) opis możliwych konsekwencji naruszenia; (d) opis środków zastosowanych lub

proponowanych w celu zaradzenia naruszeniu, w tym środków minimalizujących jego ewentualne negatywne skutki.

6.3. Jeżeli podanie wszystkich informacji w pierwszym zgłoszeniu nie jest możliwe, Podmiot przetwarzający przekazuje je sukcesywnie, bez zbędnej zwłoki, w miarę ustalania okoliczności naruszenia.

6.4. Zgłoszenie naruszenia organowi nadzorczemu oraz zawiadomienie osób, których dane dotyczą, należy do Administratora. Podmiot przetwarzający udziela Administratorowi wsparcia niezbędnego do wykonania tych obowiązków.

6.5. Podmiot przetwarzający dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia, jego skutki oraz podjęte działania zaradcze.

7. Ocena skutków i uprzednie konsultacje

7.1. Podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, udziela Administratorowi pomocy przy przeprowadzaniu oceny skutków dla ochrony danych (art. 35 RODO) oraz przy uprzednich konsultacjach z organem nadzorczym (art. 36 RODO).

7.2. Pomoc polega w szczególności na udostępnieniu opisu czynności przetwarzania, stosowanych środków bezpieczeństwa oraz wykazu Podprzetwarzających. Ocena skutków pozostaje obowiązkiem Administratora.

8. Audyt i wykazanie zgodności

8.1. Podmiot przetwarzający udostępnia Administratorowi — na jego żądanie złożone w formie dokumentowej — informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.

8.2. Administrator ma prawo do przeprowadzenia audytu, w tym inspekcji, u Podmiotu przetwarzającego, na następujących zasadach:

1. audyt może być przeprowadzony nie częściej niż **raz w roku kalendarzowym**, z zastrzeżeniem pkt 8.3;
2. Administrator zawiadamia o zamiarze przeprowadzenia audytu z co najmniej **14-dniowym wyprzedzeniem**, wskazując jego zakres, planowany czas trwania oraz osoby, które będą go przeprowadzać;
3. audyt odbywa się w Dniach roboczych, w sposób możliwie najmniej zakłócający działalność Podmiotu przetwarzającego, i nie może obejmować dostępu do danych innych klientów Podmiotu przetwarzającego ani do informacji stanowiących tajemnicę przedsiębiorstwa w zakresie wykraczającym poza cel audytu;
4. osoby przeprowadzające audyt są zobowiązane do zachowania poufności; jeżeli audyt przeprowadza podmiot zewnętrzny, nie może on być konkurentem Podmiotu przetwarzającego;
5. Strony ponoszą własne koszty audytu.

8.3. Ograniczenie częstotliwości z pkt 8.2 ppkt 1 nie ma zastosowania, gdy audyt jest następstwem stwierdzonego naruszenia ochrony danych osobowych albo jest przeprowadzany na żądanie organu nadzorczego.

8.4. Podmiot przetwarzający może wykazać spełnienie obowiązków również przez przedstawienie aktualnych certyfikatów, raportów z audytów niezależnych podmiotów lub wyników testów bezpieczeństwa, jeżeli nimi dysponuje. Administrator uwzględni takie dokumenty przy ustalaniu zakresu audytu.

9. Przekazywanie danych do państw trzecich

9.1. Podmiot przetwarzający przetwarza powierzone dane osobowe na terytorium Europejskiego Obszaru Gospodarczego.

9.2. Przekazanie danych do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie wtedy, gdy spełniony jest jeden z warunków określonych w Rozdziale V RODO — w szczególności gdy Komisja Europejska stwierdziła odpowiedni stopień ochrony albo gdy zastosowano standardowe klauzule umowne wraz z oceną skutków przekazania i niezbędnymi środkami uzupełniającymi.

9.3. Podmiot przetwarzający informuje Administratora o każdym planowanym przekazaniu danych poza EOG na zasadach i w terminach określonych w pkt 4.3, a Administratorowi przysługują wówczas uprawnienia opisane w pkt 4.4.

10. Usunięcie lub zwrot danych

10.1. Po zakończeniu świadczenia Usługi Podmiot przetwarzający — zależnie od decyzji Administratora — zwraca mu powierzone dane osobowe albo je usuwa, wraz z wszelkimi ich istniejącymi kopiami.

10.2. Przed wygaśnięciem Umowy Administrator może samodzielnie wyeksportować dane z Usługi, w zakresie i formatach wskazanych w Karcie Produktowej. Brak wykonania eksportu przez Administratora nie wstrzymuje usunięcia danych.

10.3. Po wygaśnięciu Umowy dane pozostają w systemach Podmiotu przetwarzającego przez **okres karencji** wskazany w Karcie Produktowej, w stanie niedostępnym dla Administratora. W tym okresie Administrator może zgłosić żądanie wydania kopii bazy danych Instancji Klienta; wydanie kopii jest odpłatne i następuje po uregulowaniu wszystkich wymagalnych należności.

10.4. Po upływie okresu karencji dane są trwale usuwane, a kopie zapasowe zawierające te dane — usuwane wraz z upływem cyklu retencji kopii wskazanego w Karcie Produktowej. Na żądanie Administratora Podmiot przetwarzający potwierdza usunięcie danych w formie dokumentowej.

10.5. Podmiot przetwarzający może zachować dane osobowe po zakończeniu Umowy wyłącznie w zakresie i przez okres, w jakim wymagają tego przepisy prawa Unii lub prawa państwa członkowskiego (w szczególności przepisy podatkowe i o rachunkowości), przy zachowaniu środków bezpieczeństwa opisanych w Załączniku B i wyłącznie w celu wynikającym z tych przepisów.

10.6. Wpisy w dzienniku audytu, dokumentujące operacje wykonane w Usłudze, są rekordami niemodyfikowalnymi i podlegają usunięciu wraz z całością danych Instancji Klienta, z zastrzeżeniem pkt 10.5.

11. Odpowiedzialność

11.1. Każda ze Stron odpowiada za szkody spowodowane przetwarzaniem na zasadach określonych w art. 82 RODO.

11.2. Administrator odpowiada za: legalność powierzonych danych i istnienie podstawy prawnej ich przetwarzania, prawidłowość i adekwatność zakresu danych wprowadzanych do Usługi, wykonanie obowiązku informacyjnego wobec osób, których dane dotyczą, oraz za konfigurację uprawnień Użytkowników w Instancji Klienta.

11.3. Administrator zobowiązuje się nie wprowadzać do Usługi danych osobowych w zakresie szerszym niż niezbędny do celów, dla których korzysta z Usługi. Jeżeli Administrator wprowadza do Usługi dane szczególnych kategorii w rozumieniu art. 9 RODO lub dane dotyczące wyroków skazujących i czynów zabronionych (art. 10 RODO), odpowiada wyłącznie za istnienie podstawy prawnej takiego przetwarzania oraz za zastosowanie środków adekwatnych do podwyższonego ryzyka.

11.4. Ograniczenie odpowiedzialności Podmiotu przetwarzającego wynikające z Regulaminu nie ma zastosowania do odpowiedzialności wobec osób, których dane dotyczą, ani do administracyjnych kar pieniężnych nałożonych na Podmiot przetwarzający.

12. Postanowienia końcowe

12.1. Umowa powierzenia obowiązuje przez okres obowiązywania Umowy. Postanowienia Rozdziałów 10 i 11 pozostają w mocy także po jej wygaśnięciu.

12.2. Zmiana Umowy powierzenia następuje w trybie właściwym dla zmiany Regulaminu, z zastrzeżeniem że zmiany wynikające wprost ze zmiany przepisów prawa lub z wytycznych organu nadzorczego wchodzą w życie z dniem wskazanym przez Podmiot przetwarzający, nie wcześniej niż z dniem, od którego obowiązują te przepisy lub wytyczne. Zmiana wykazu Podprzetwarzających (Załącznik C) następuje w trybie z pkt 4.3–4.4 i nie stanowi zmiany Umowy powierzenia.

12.3. W sprawach nieuregulowanych stosuje się RODO, ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych oraz postanowienia Regulaminu.

12.4. W razie sprzeczności pomiędzy Umową powierzenia a Regulaminem — w zakresie przetwarzania danych osobowych — pierwszeństwo ma Umowa powierzenia.

12.5. Kontakt w sprawach ochrony danych osobowych po stronie Podmiotu przetwarzającego: rodo@ite.pl.

Załącznik A — Opis przetwarzania

A.1. Przedmiot przetwarzania: świadczenie Usługi polegającej na udostępnieniu Administratorowi oprogramowania IT Excellence w modelu SaaS, w zakresie wynikającym z Zamówienia.

A.2. Czas trwania przetwarzania: okres obowiązywania Umowy, powiększony o okres karencji wskazany w Karcie Produktowej.

A.3. Charakter i cel przetwarzania: przechowywanie, porządkowanie, utrwalanie, modyfikowanie, przeglądanie, wykorzystywanie, udostępnianie Użytkownikom Administratora oraz usuwanie danych — w zakresie niezbędnym do realizacji funkcji Oprogramowania, jego utrzymania, usuwania Usterek i zapewnienia bezpieczeństwa.

A.4. Kategorie osób i danych — wspólne dla wszystkich Usług:

Kategoria osób	Kategorie danych	Uwagi
Użytkownicy Administratora	imię, nazwisko, służbowy adres e-mail (login), numer telefonu, stanowisko, przypisane role i uprawnienia, przypisanie do firm i jednostek organizacyjnych, skrót hasła, sekret uwierzytelniania dwuskładnikowego, dane o aktywności w systemie (logowania, wykonane operacje)	Skrót hasła oraz sekret 2FA nie są przechowywane w postaci jawnej
Osoby kontaktowe kontrahentów Administratora	imię, nazwisko, stanowisko, adres e-mail, numer telefonu, przypisanie do kontrahenta, notatki i historia kontaktów	—
Osoby fizyczne prowadzące działalność gospodarczą, będące kontrahentami	firma, adres, NIP, REGON, numery rachunków bankowych, dane kontaktowe, historia współpracy, stan rozrachunków	Dane przedsiębiorcy będącego osobą fizyczną stanowią dane osobowe

Kategoria osób	Kategorie danych	Uwagi
Pracownicy Administratora (jeżeli Administrator korzysta z kartoteki pracowników lub modułów kadrowych)	imię, nazwisko, data i miejsce urodzenia, **numer PESEL**, seria i numer dokumentu tożsamości, adres zamieszkania i korespondencyjny, dane kontaktowe, stanowisko, jednostka organizacyjna, dane dotyczące zatrudnienia, przełożony	Numer PESEL i numer dokumentu tożsamości są szyfrowane w bazie danych (Załącznik B, pkt B.3)
Osoby wskazane w dokumentach wprowadzonych do Usługi	dane zawarte w treści i załącznikach dokumentów — zakres ustala wyłącznie Administrator	Podmiot przetwarzający nie ma wpływu na zakres tych danych
Osoby, których dane Administrator wprowadzi w polach dodatkowych, tabelach dodatkowych lub modułach własnych	zakres definiowany samodzielnie przez Administratora w kreatorze	Odpowiedzialność za adekwatność zakresu spoczywa na Administratorze (pkt 11.3)

A.5. Kategorie dodatkowe — Usługa eHandel365:

Kategoria osób	Kategorie danych	Uwagi
Nabywcy i odbiorcy będący osobami fizycznymi prowadzącymi działalność gospodarczą	dane identyfikacyjne i adresowe, NIP, dane kontaktowe, historia transakcji, stan rozrachunków	—
Osoby wskazane na dokumentach handlowych i dokumentach dostawy	imię i nazwisko osoby odbierającej towar lub wystawiającej dokument, podpis odbioru, dane kontaktowe do dostawy	Zakres ustala Administrator przez konfigurację typów dokumentów
Przedstawiciele handlowi korzystający z aplikacji mobilnej	dane Użytkownika (wiersz 1 tabeli A.4) oraz dane o aktywności sprzedażowej: wystawione dokumenty, obsłużeni kontrahenci, zrealizowane dostawy	Usługa nie zbiera danych o lokalizacji urządzenia

A.6. Szczególne kategorie danych (art. 9 RODO): Usługa **nie jest przeznaczona** do przetwarzania danych szczególnych kategorii. Jeżeli Administrator korzysta z modułów kadrowych (w szczególności e-teczki, BHP, zaświadczeń) i wprowadza do nich dane dotyczące zdrowia — na przykład orzeczenia lekarskie lub zaświadczenia o badaniach — przetwarzanie takich danych odbywa się wyłącznie na jego odpowiedzialność, na zasadach opisanych w pkt 11.3 Umowy powierzenia.

A.7. Odbiorcy danych wynikający z funkcji Usługi: jeżeli Administrator korzysta z integracji z Krajowym Systemem e-Faktur, dane zawarte w fakturach są przekazywane do KSeF. Administratorem danych w KSeF jest Szef Krajowej Administracji Skarbowej, a przekazanie następuje na podstawie obowiązku prawnego ciążącego na Administratorze, nie zaś na podstawie niniejszej Umowy powierzenia.

A.8. Lokalizacja przetwarzania: Europejski Obszar Gospodarczy. Szczegóły — Karta Produktowa i Załącznik C.

Załącznik B — Środki techniczne i organizacyjne (art. 32 RODO)

Podmiot przetwarzający stosuje co najmniej następujące środki. Wykaz odzwierciedla stan na dzień wskazany w nagłówku Umowy powierzenia; Podmiot przetwarzający może zastępować poszczególne środki innymi, zapewniającymi nie niższy poziom bezpieczeństwa.

B.1. Kontrola dostępu do systemu. Dostęp do Usługi wymaga indywidualnego konta Użytkownika i uwierzytelnienia. Hasła są przechowywane wyłącznie w postaci skrótu kryptograficznego z solą; hasła jawne

nie są zapisywane ani logowane. Wymuszana jest polityka złożoności haseł. Liczba prób logowania oraz prób odgadnięcia kodów jednorazowych jest ograniczana automatycznie.

B.2. Uwierzytelnianie dwuskładnikowe. Usługa udostępnia uwierzytelnianie dwuskładnikowe oparte na jednorazowych kodach czasowych (TOTP). Dla kont o uprawnieniach administracyjnych jego stosowanie jest wymagane. Sesje są zabezpieczone tokenami podpisywanymi kryptograficznie, z rotacją tokenów odświeżających i automatycznym wykrywaniem ich ponownego użycia.

B.3. Szyfrowanie. Transmisja danych pomiędzy urządzeniem Użytkownika a Usługą jest szyfrowana protokołem TLS. Wybrane kategorie danych — numer PESEL, seria i numer dokumentu tożsamości oraz sekret uwierzytelniania dwuskładnikowego — są dodatkowo szyfrowane na poziomie kolumn bazy danych; klucz szyfrujący jest przechowywany poza bazą danych.

B.4. Rozdzielenie danych klientów. Dane każdego klienta są utrzymywane w wydzielonej przestrzeni logicznej (odrębny schemat lub odrębna baza danych). Warstwa aplikacji rozstrzyga przynależność żądania do konkretnego klienta przed jakimkolwiek dostępem do danych.

B.5. Kontrola uprawnień. Dostęp do poszczególnych funkcji i danych jest kontrolowany modelem ról i uprawnień o ziarnistości pojedynczej operacji na pojedynczym typie danych, z zakresami ograniczającymi widoczność (dane własne / jednostki organizacyjnej / firmy / wszystkie). Konfiguracja uprawnień pozostaje w gestii Administratora.

B.6. Rozliczalność. Każda operacja modyfikująca dane jest rejestrowana w dzienniku audytu obejmującym: identyfikator Użytkownika, rodzaj operacji, identyfikator rekordu oraz znacznik czasu. Wpisy dziennika są niemodyfikowalne. Do dziennika nie są zapisywane dane wrażliwe w postaci jawnej — w szczególności numery PESEL, hasła ani sekrety uwierzytelniające.

B.7. Usuwanie i retencja. Usunięcie rekordu przez Użytkownika ma charakter logiczny i jest odwracalne przez uprawnionego Użytkownika. Trwałe usunięcie danych następuje automatycznie po upływie okresu retencji, konfigurowalnego przez Administratora. Realizacja prawa do bycia zapomnianym obejmuje anonimizację danych identyfikujących przy zachowaniu rozliczalności operacji historycznych.

B.8. Kopie zapasowe. Kopie zapasowe bazy danych są wykonywane automatycznie, z częstotliwością i okresem przechowywania wskazanymi w Karcie Produktowej. Kopie są przechowywane w infrastrukturze objętej tymi samymi środkami bezpieczeństwa co środowisko produkcyjne.

B.9. Rozdzielenie środowisk. Środowiska deweloperskie i testowe są odseparowane od produkcyjnego. Dane produkcyjne nie są wykorzystywane w środowiskach nieprodukcyjnych bez uprzedniej anonimizacji.

B.10. Zarządzanie podatnościami. Podmiot przetwarzający monitoruje podatności wykorzystywanych komponentów i bibliotek oraz wdraża poprawki bezpieczeństwa w terminach adekwatnych do poziomu ryzyka. Zmiany w Oprogramowaniu przechodzą automatyczną kontrolę jakości przed wdrożeniem na środowisko produkcyjne.

B.11. Dostęp personelu Podmiotu przetwarzającego. Dostęp personelu Podmiotu przetwarzającego do danych Administratora jest ograniczony do przypadków niezbędnych do świadczenia Usługi — w szczególności do diagnozy zgłoszonej Usterki — udzielany na zasadzie minimalnych uprawnień i rejestrowany. Personel jest zobowiązany do zachowania poufności i przechodzi szkolenia z ochrony danych osobowych.

B.12. Ciągłość działania. Podmiot przetwarzający utrzymuje zdolność do przywrócenia dostępności danych i dostępu do nich w razie incydentu fizycznego lub technicznego, w terminie adekwatnym do charakteru Usługi, oraz okresowo weryfikuje skuteczność procedury odtworzenia z kopii zapasowej.

Załącznik C — Wykaz Podprzetwarzających

Aktualny wykaz jest publikowany pod adresem https://ite.pl/podprzetwarzajacy i aktualizowany w trybie opisanym w pkt 4.3–4.4 Umowy powierzenia.

Podprzetwarzający	Rola / zakres przetwarzania	Lokalizacja przetwarzania
Microsoft	dostawca infrastruktury serwerowej (hosting Usługi, przechowywanie kopii zapasowych)	Polska
Microsoft Ireland Operations Limited	dostawca poczty elektronicznej (wysyłka wiadomości transakcyjnych)	Irlandia (EOG)

Do uzupełnienia przed publikacją. Wykaz musi obejmować wszystkie podmioty mające faktyczny dostęp do danych Administratora — w szczególności dostawcę infrastruktury, dostawcę poczty transakcyjnej (SMTP), dostawcę usług monitoringu i logowania błędów, zewnętrznych wykonawców utrzymania oraz — jeżeli Usługa korzysta z funkcji opartych na sztucznej inteligencji — dostawcę tych usług. Wykaz musi być spójny z Kartą Produktową (pozycja „Podwykonawcy").

Umowa powierzenia przetwarzania danych osobowych — IT Excellence · Załącznik nr 2 — DPA · wersja wrzesień 2026 · © IT Excellence S.A.

Uwaga: dokument nie był weryfikowany przez radcę prawnego — przed publikacją wymaga przeglądu prawnego.