

Umowa powierzenia przetwarzania danych osobowych: BudOS

Nr dokumentu: DPA-BUDOS-2026-001

Wersja: 2.1

Publikacja: 05.10.2026.

Powiązane: [Regulamin](#), [Polityka prywatności](#), [Licencja](#), [Klauzula AI](#), [Polityka cookies](#).

§1. Strony, role i zawarcie

- Klient** to podmiot wskazany w skutecznie przyjętym zamówieniu lub umowie o usługę BudOS, będący administratorem danych powierzonych („Administrator”) albo podmiotem przetwarzającym na rzecz innego administratora, jeżeli ma udokumentowane uprawnienie do dalszego powierzenia i udzielania instrukcji. W drugim przypadku QA10 jest kolejnym podmiotem przetwarzającym w łańcuchu, a Klient wykonuje wobec QA10 prawa i obowiązki z DPA w granicach swojego umocowania. Nie pozbawia to pierwotnego administratora praw wynikających z RODO. O roli decyduje rzeczywista czynność przetwarzania, a nie nazwa konta lub status przedsiębiorcy.
- QA10 sp. z o.o.**, ul. Mariacka 37, 40-014 Katowice, KRS 0001232199, NIP 9542906279, REGON 544435060, kapitał zakładowy 5 000 zł, wpisana do rejestru przedsiębiorców KRS prowadzonego przez Sąd Rejonowy Katowice-Wschód w Katowicach, VIII Wydział Gospodarczy KRS, jest podmiotem przetwarzającym w zakresie Załącznika 1. Kontakt spółki: **hello@qa10.io**; zgłoszenia naruszeń i incydentów: **Pomoc@budos.io**. Sposób reprezentacji ujawniony w KRS wymaga przy wieloosobowym zarządzie współdziałania dwóch członków zarządu albo członka zarządu z prokurentem. Zawarcie DPA wymaga zachowania właściwej reprezentacji i warunków ust. 3.
- DPA wiąże strony wyłącznie po skutecznym zawarciu w formie pisemnej, w tym elektronicznej w rozumieniu art. 28 ust. 9 RODO, oraz ustaleniu i utrwaleniu stron, ich ról, wersji dokumentu, czasu zawarcia i uzgodnionych warunków. Może dotyczyć także konsumenta lub chronionej JDG, o ile rzeczywiście dochodzi do powierzenia. **Przed przyjęciem danych wymagających powierzenia strony muszą uzgodnić konkretny zakres Załącznika 1, prawidłowo uzupełnić i zatwierdzić Załącznik 2 oraz ustalić środki właściwe dla tego zakresu zgodnie z Załącznikiem 3.** Zamówienie i przyjęte załączniki muszą pozwalać ustalić, na co strony się umówiły, i zachować tę treść. Założenie konta, zapoznanie się z Polityką prywatności lub wybór narzędzia nie zastępują uzgodnienia i zatwierdzenia zakresu oraz załączników; samo udostępnienie DPA na stronie nie zawiera umowy. Akceptacja DPA i Regulaminu nie jest zgodą z art. 6 ust. 1 lit. a RODO; zapoznanie się z Polityką prywatności nie wymaga udzielenia zgody na jej treść. Odrębne aneksy wymagają formy i reprezentacji przewidzianych prawem i

umową. Do czasu spełnienia warunków QA10 nie przyjmuje danych wymagających powierzenia na podstawie niniejszej DPA, a Klient nie powinien ich przekazywać.

4. QA10 jest odrębnym administratorem operacji, których cele i istotne środki samodzielnie ustala, w szczególności własnych rozliczeń, relacji z Klientem i odpowiednich czynności zabezpieczania usługi. Informuje o nich [Polityka prywatności](#). DPA nie przenosi na Klienta odpowiedzialności za własne cele QA10 i nie zezwala na używanie danych powierzonych do marketingu, trenowania modeli, analityki między klientami ani niezależnych celów operatorów AI. Własne pozyskiwanie i opracowywanie publicznych źródeł przez QA10, newsletter oraz marketing witryny są odrębnymi operacjami, a nie powierzeniem przez każdego odbiorcę BudOS. Gdy prywatny użytkownik nie działa jako administrator powierzający dane, jego własne dane konta podlegają Polityce prywatności, a nie DPA tylko z racji posiadania konta.

§2. Przedmiot, czas i instrukcje

1. Przedmiot, czas, charakter i cele przetwarzania, rodzaje danych, kategorie osób oraz obowiązki i uprawnienia Klienta określa **Załącznik 1**, stanowiący integralną część DPA wraz z uzgodnionym zakresem zamówienia. QA10 przetwarza dane wyłącznie na udokumentowane polecenia Klienta, także dotyczące przekazania do państwa trzeciego lub organizacji międzynarodowej. Wyjątkiem jest obowiązek wynikający z prawa Unii lub państwa członkowskiego właściwego dla QA10; QA10 informuje o nim Klienta przed przetwarzaniem, chyba że prawo zakazuje takiej informacji z ważnych względów interesu publicznego.
2. Instrukcję może stanowić skutecznie zawarta DPA z załącznikami i zamówieniem, pisemne lub elektroniczne polecenie przekazane uzgodnionym kanałem albo czynność uprawnionego Użytkownika w zatwierdzonej funkcji Serwisu, w granicach uzgodnionego zakresu i prawa. Strony utrzymują możliwość ustalenia treści i pochodzenia instrukcji. Samo udostępnienie przycisku, podłączenie integracji lub techniczne przełączenie na trasę zastępczą nie zmienia istotnych celów, kategorii danych, odbiorców, państw transferu ani warunków retencji. Taka zmiana wymaga odpowiedniej udokumentowanej instrukcji, upoważnienia oraz, gdy jest to konieczne, skutecznej zmiany umowy.
3. Jeżeli zdaniem QA10 instrukcja narusza RODO lub inne unijne albo krajowe przepisy o ochronie danych, QA10 **niezwłocznie informuje Klienta**, wskazuje przyczynę i wstrzymuje sporną operację w zakresie niezbędnym do wyjaśnienia, chyba że wiążące prawo wymaga innego działania. QA10 nie ma obowiązku wykonywać bezprawnej instrukcji. Pozostałe zgodne z prawem czynności mogą być kontynuowane; wstrzymanie nie znosi obowiązków zabezpieczenia, pomocy, zwrotu i usunięcia danych.
4. Klient ustala własne cele i podstawy prawne z art. 6 oraz, gdy mają zastosowanie, art. 9 lub 10 RODO. Odpowiada za zgodność instrukcji, minimalizację danych, ich niezbędność i okresy przechowywania dla swoich celów, obowiązki informacyjne wobec osób, także przy danych ze źródeł publicznych, oraz uprawnienia w łańcuchu powierzenia. Publiczna dostępność dokumentu nie oznacza, że zawarte w nim dane są anonimowe

lub mogą być przetwarzane bez podstawy. Obowiązki Klienta nie uchylają własnych obowiązków QA10 z art. 28–32 RODO i DPA.

5. Klient wskazuje osoby uprawnione do udzielania instrukcji i ich zakres umocowania, chroni dane logowania oraz aktualizuje uprawnienia Użytkowników. QA10 może proporcjonalnie zweryfikować pochodzenie instrukcji przed ujawnieniem lub usunięciem danych. Instrukcja wykraczająca poza uzgodniony zakres wymaga ustalenia wykonalności, ryzyka i ewentualnej zmiany zamówienia. Brak uzgodnienia dodatkowego świadczenia nie uprawnia do odmowy obowiązków wynikających z RODO lub już zawartej DPA.

§3. Poufność i bezpieczeństwo

1. QA10 dopuszcza do danych wyłącznie osoby upoważnione w zakresie niezbędnym do ich zadań, zobowiązane do poufności albo objęte odpowiednim ustawowym obowiązkiem poufności. Obowiązek zachowania poufności danych trwa także po zakończeniu dostępu. QA10 zapewnia szkolenie odpowiednie do zadań, nadawanie, przegląd i odbieranie uprawnień oraz kontrolę czynności osób działających pod jej władztwem. Niniejszy paragraf nie zmienia odrębnych zasad ochrony Informacji Poufnych i tajemnic przedsiębiorstwa z Regulaminu i Licencji.
2. QA10 jest zobowiązana zapewnić środki wymagane art. 32 RODO, z uwzględnieniem stanu wiedzy technicznej, kosztu wdrożenia, charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka dla praw i wolności osób. Minimalne wymagania i sposób ich udokumentowania określa **Załącznik 3**. Przed powierzeniem QA10 udostępnia Klientowi opis środków właściwych dla uzgodnionego zakresu, a następnie utrzymuje ich skuteczność i poddaje je odpowiednim przeglądom. Informuje o istotnym obniżeniu poziomu ochrony przed wprowadzeniem zmiany; jeżeli pilna zmiana jest niezbędna do usunięcia zagrożenia, przekazuje informację bez zbędnej zwłoki po jej zastosowaniu. Zmiana nie może prowadzić do przetwarzania niezgodnego z prawem.
3. QA10 nie wykorzystuje danych powierzonych w środowiskach testowych i nie przekazuje treści dokumentów, promptów ani wyników do nieupoważnionych modeli, analityki lub wtyczek. Dane przekazywane zewnętrznemu AI podlegają minimalizacji i ograniczeniu do zatwierdzonej operacji. Dostęp wsparcia do treści Klienta ogranicza się do niezbędnego zakresu i dokumentuje. Środki bezpieczeństwa są obowiązkiem umownym, a nie zapewnieniem bezwzględnej odporności na każde zagrożenie; nie wyłącza to odpowiedzialności QA10 za ich niewykonanie.

§4. Dalsi procesorzy i zmiany

1. QA10 może zlecić przetwarzanie innemu odrębnemu podmiotowi **dopiero po uprzednim szczególnym lub ogólnym pisemnym upoważnieniu Klienta** i skutecznym związaniu tego podmiotu umową lub aktem prawnym nakładającym co najmniej te same obowiązki ochrony danych w odpowiednim zakresie, zgodnie z art. 28 ust. 2 i 4 RODO. QA10 pozostaje wobec Klienta w pełni odpowiedzialna za wykonanie obowiązków ochrony

danych przez dalszego procesora. Własne API QA10, procesy przetwarzania i używane oprogramowanie nie są odrębnymi osobami prawnymi. Operator płatności działający dla własnych rozliczeń nie staje się przez to dalszym procesorem treści Klienta.

2. Przed upoważnieniem Klient otrzymuje konkretny, aktualny wykaz rzeczywistych dalszych procesorów z ich tożsamością prawną, rolą, funkcją, zakresem danych i czynności, krajami i regionami przetwarzania oraz zweryfikowanym mechanizmem transferu poza EOG, jeżeli jest wymagany. Konkretna wersja wykazu w Załączniku 2 musi zostać prawidłowo uzupełniona, skutecznie udostępniona i zatwierdzona przed powierzeniem; do tego czasu żaden podmiot nie jest upoważniony na jego podstawie. W przypadku bramki AI wykaz obejmuje również rzeczywistych operatorów endpointów przetwarzających dane. Nazwa modelu, biblioteki, domeny lub regionu w konfiguracji nie identyfikuje całego łańcucha i nie zastępuje upoważnienia.
3. Przy skutecznie udzielonym upoważnieniu ogólnym QA10 przekazuje Klientowi **aktywną wiadomość co najmniej 14 dni kalendarzowych przed** dodaniem, zastąpieniem albo istotnym rozszerzeniem czynności dalszego procesora. Zawiadomienie trafia na uzgodniony adres kontaktowy i zawiera informacje z ust. 2, podstawę transferu, datę planowanej zmiany oraz sposób sprzeciwu; sama zmiana strony internetowej nie wystarcza. Klient może w tym terminie zgłosić uzasadniony względami ochrony danych sprzeciw na **hello@qa10.io**. QA10 rozpatruje sprzeciw i proponuje rozwiązanie, zależnie od wykonalności: zachowanie dotychczasowej ścieżki, alternatywę bez nowego procesora, wstrzymanie danej funkcji albo zakończenie odpowiedniego świadczenia na zasadach Regulaminu i prawa, z zachowaniem zwrotu i eksportu danych. **Do czasu rozwiązania sprzeciwu QA10 nie kieruje danych do kwestionowanego podmiotu.** Nie jest zobowiązana utrzymywać technicznie niedostępnej ścieżki ani tworzyć nowej funkcji poza zakresem umowy i prawa. Milczenie może mieć skutek wyłącznie w granicach wcześniej skutecznie udzielonego upoważnienia ogólnego i udokumentowanego skutecznego zawiadomienia. Nie zastępuje szczególnego upoważnienia, gdy jest ono wymagane, ani warunków transferu i bezpieczeństwa.
4. QA10 zapewnia przekazanie w dalszym łańcuchu obowiązków dotyczących instrukcji, poufności, bezpieczeństwa, pomocy, zawiadamiania o naruszeniach, zwrotu i usunięcia oraz wykazania zgodności i audytu. Utrzymuje dokumentację umów, wersji wykazu, zawiadomień, sprzeciwów i upoważnień. Publiczne warunki dostawcy ani oznaczenie ZDR nie zastępują skutecznego związania obowiązkami z art. 28 ust. 4 RODO.

§5. Przekazanie poza EOG i AI

1. Przed przekazaniem danych do państwa trzeciego lub organizacji międzynarodowej, także przez zdalny dostęp, wsparcie, sieć dostarczania treści, logi lub kopie, QA10 identyfikuje odbiorców i role oraz zapewnia właściwy mechanizm z rozdziału V RODO dla każdej ścieżki. Może to być decyzja o adekwatności z art. 45 w rzeczywistym zakresie objętego nią odbiorcy albo odpowiednie zabezpieczenie z art. 46, w tym skutecznie zawarte standardowe klauzule umowne we właściwym module. QA10 dokumentuje ocenę skuteczności zabezpieczeń i, gdy są potrzebne, środki dodatkowe.

Na żądanie udostępnia Klientowi informacje i dostępne kopie zabezpieczeń z proporcjonalną ochroną danych innych osób i tajemnic. Nie obowiązuje ogólny zakaz przetwarzania poza EOG, lecz bez spełnienia warunków QA10 nie dokonuje transferu danych powierzonych przez niezatwierdzoną ścieżkę. Lokalizacja serwera nie zastępuje podstawy transferu, a umowy w łańcuchu muszą skutecznie wiązać właściwe podmioty w wymaganym zakresie.

2. **BudOS ma skonfigurowaną ścieżkę AI przez OpenRouter.** Ogólna konfiguracja przewiduje Grok 4.7 (x-ai/grok-4.7) do analizy, rozmowy, generowania dokumentów i zadań mogących obejmować dane osobowe oraz DeepSeek V4.1 Flash (deepseek/deepseek-v4.1-flash) do klasyfikacji zadeklarowanej jako nieobejmująca danych osobowych. Deklaracja nieosobowego charakteru lub techniczne usunięcie niektórych identyfikatorów nie gwarantują anonimizacji. Dopuszczenie OpenRouter i operatorów modeli do danych konkretnego Klienta wymaga uprzedniego upoważnienia, ustalenia krajów przetwarzania i spełnienia warunków ochrony danych dla danej operacji. Przed użyciem danych powierzonych QA10 musi zapewnić skuteczne umowy całego łańcucha, upoważnienia, legalność transferów, właściwe ustawienia i wykluczenie niezatwierdzonych ścieżek zastępczych, wtyczek oraz przechowywania plików. **Brak treningu na danych Klienta, zatwierdzony zakres nieutrwalania treści przez operatora inferencji oraz zatrzymanie operacji przy braku zgodnej ścieżki pozostają warunkami świadczenia.** Ogólny tor AI nie jest objęty zapewnieniem ZDR ani automatycznego zatrzymania wszystkich alternatywnych tras. Danych powierzonych nie wolno do niego kierować przed spełnieniem powyższych warunków dla konkretnej operacji. Bezpośrednia umowa QA10 z każdym operatorem nie jest automatycznie konieczna, jeżeli właściwe obowiązki są skutecznie nałożone w całym łańcuchu; QA10 musi jednak wykazać ten skutek przed przekazaniem danych.
3. Żadna bezpośrednia lub awaryjna ścieżka do innego operatora nie jest upoważniona przez samą konfigurację OpenRouter, błąd usługi ani wybór przycisku przez Użytkownika. Każda ścieżka zastępcza wymaga uprzedniego ustalenia roli, skutecznej umowy, upoważnienia, zakresu nieutrwalania, retencji i mechanizmu transferu. **Gdy nie ma ścieżki spełniającej te warunki, QA10 jest zobowiązana zatrzymać daną operację i nie kierować danych niejawnie do innego odbiorcy.** Pozostałe zgodne z prawem funkcje mogą działać.
4. QA10 nie używa danych powierzonych do własnego trenowania lub dostrajania modeli i nie kieruje ich do treningu operatorów. Zatwierdzony endpoint inferencji ma zapewniać **nieutrwalanie treści promptów i odpowiedzi przez operatora (ZDR)**, a nie tylko zakaz treningu. Preferencja data_collection=deny nie zastępuje wymogu nieutrwalania treści przez operatora inferencji. Zakres ZDR wymaga odrębnej weryfikacji dla funkcji, operatora i endpointu. Nie oznacza automatycznie braku metadanych technicznych lub rozliczeniowych, przechowywania dokumentów i wyników w Organizacji Klienta, logów QA10, przetwarzania przez bramkę, narzędzia lub wtyczki. Te odrębne operacje muszą mieć uzgodniony, niezbędny zakres, odbiorców, retencję i zabezpieczenia, bez użycia danych powierzonych do niezależnych celów. Nie wolno w ten sposób obchodzić zakazu utrwalania treści u operatora inferencji. Brak właściwej umowy lub zgodnego

endpointu oznacza wstrzymanie przetwarzania AI danych powierzonych. Minimalizacja nie zastępuje tych warunków.

5. Pomoc AI jest odrębną funkcją doboru fragmentów centrum pomocy, a nie poleceniem analizy dokumentów Organizacji. Jej konfiguracja przewiduje OpenRouter z wyborem DeepInfra i modelem DeepSeek V4.1 Flash, odrębnie od ogólnej analizy i generowania dokumentów. W pytaniu nie należy umieszczać danych osobowych, haseł, kluczy ani poufnych dokumentów; należy opisać ekran i czynność. Samo wpisanie danych do pytania nie upoważnia nowego odbiorcy. Jeżeli pytanie obejmuje dane powierzone, QA10 nadal podlega warunkom DPA i nie może uznać ich za nieosobowe tylko dlatego, że są w rozmowie z pomocą. W sprawach wymagających przekazania danych lub kontaktu z człowiekiem należy użyć **Pomoc@budos.io**, ograniczając treść do potrzebnego zakresu i uzgadniając bezpieczny kanał dla załączników. Przetwarzanie danych powierzonych przez pomoc AI wymaga imiennego upoważnienia odbiorców i skutecznych umów w jej łańcuchu.

§6. Prawa osób, pomoc i obowiązki Klienta

1. QA10 nie udziela samodzielnej odpowiedzi w imieniu Klienta na żądanie dotyczące danych powierzonych, chyba że otrzymała jego instrukcję lub prawo wymaga innego działania. Niezwłocznie przekazuje Klientowi otrzymane żądanie. Z uwzględnieniem charakteru przetwarzania i w miarę możliwości zapewnia odpowiednie środki techniczne i organizacyjne pomagające Klientowi wykonywać obowiązki z art. 12–22 RODO, w tym dotyczące dostępu i kopii, sprostowania, usunięcia, ograniczenia, informacji o odbiorcach zmian, przenoszenia i sprzeciwu oraz decyzji z art. 22. Udostępnia potrzebne dane i informacje o odbiorcach; publiczne pochodzenie danych nie jest podstawą odmowy pomocy.
2. QA10 pomaga Klientowi w zapewnieniu bezpieczeństwa i wykonaniu obowiązków z art. 32–36 RODO, w tym ocenie i dokumentowaniu naruszeń, zawiadomieniu organu i osób, ocenie skutków dla ochrony danych oraz uprzedniej konsultacji. Zakres pomocy uwzględnia charakter przetwarzania i informacje dostępne QA10. QA10 przekazuje opis czynności, środków, odbiorców i transferów potrzebny do oceny ryzyka. Dane z art. 9 lub 10 wymagają odrębnej analizy podstawy i ochrony; samo ich przypadkowe otrzymanie nie wyłącza obowiązków procesora.
3. Klient zapewnia aktualny kontakt zdolny odbierać zawiadomienia o bezpieczeństwie i dalszych procesorach, przekazuje niezbędne informacje do realizacji pomocy, utrzymuje zgodne z prawem instrukcje oraz określa wybór zwrotu lub usunięcia. Gdy jest procesorem, zapewnia współpracę z właściwym administratorem w granicach swojego umocowania. Brak kontaktu lub współpracy nie zwalnia QA10 z własnych obowiązków, w szczególności właściwego zawiadomienia dostępnym kanałem.

§7. Naruszenia

1. Po **stwierdzeniu naruszenia ochrony danych powierzonych** QA10 zawiadamia Klienta **bez zbędnej zwłoki, najpóźniej w ciągu 24 godzin**, na uzgodniony adres bezpieczeństwa lub administratora konta, a jeśli go nie wskazano, na dostępny adres kontaktowy Klienta. Nie czeka na ukończenie analizy, ustalenie liczby osób ani potwierdzenie dostawcy. Pierwsza wiadomość zawiera dostępne fakty, czas stwierdzenia, znany zakres i kontakt do dalszej współpracy. Brakujące informacje przekazuje etapami bez dalszej nieuzasadnionej zwłoki. Zgłoszenia kierowane do QA10: **Pomoc@budos.io**.
2. W miarę dostępności QA10 przekazuje opis charakteru naruszenia, kategorie i przybliżone liczby osób oraz rekordów, prawdopodobne następstwa i środki zastosowane lub proponowane do usunięcia naruszenia i ograniczenia skutków. Współpracuje przy zabezpieczeniu śladów, ograniczeniu szkody i dokumentuje naruszenie oraz podjęte działania. Klient jako administrator ocenia obowiązki z art. 33 RODO, w tym co do zasady 72 godziny od stwierdzenia, chyba że ryzyko jest mało prawdopodobne, i art. 34 RODO przy wysokim ryzyku; jako procesor przekazuje informacje właściwemu administratorowi. QA10 nie przesądza za Klienta jego obowiązku zawiadomienia, z zastrzeżeniem własnych obowiązków prawnych. Zawiadomienie nie jest samo w sobie uznaniem roszczenia lub wszystkich przyczyn naruszenia i nie ogranicza praw Klienta ani osób.

§8. Informacje, audyty i inspekcje

1. QA10 udostępnia Klientowi wszystkie informacje niezbędne do wykazania zgodności z art. 28 RODO oraz **umożliwia i przyczynia się do audytów, w tym inspekcji**, prowadzonych przez Klienta lub upoważnionego przez niego audytora. Dokumentacja, ankieta, raport niezależny lub certyfikat mogą być pierwszym etapem weryfikacji, ale nie zastępują potrzebnej inspekcji ani nie ograniczają kompetencji organu nadzorczego.
2. Zwykłą kontrolę strony planują z rozsądnym wyprzedzeniem, przykładowo 7 dni roboczych, uzgadniając zakres związany z danymi Klienta i zgodnością powierzenia, harmonogram, sposób dostępu i poufność audytora. Kontrola powinna proporcjonalnie chronić ciągłość usługi, bezpieczeństwo, dane innych klientów oraz rzeczywiste tajemnice QA10 i osób trzecich. Ochronę zapewnia się przez ograniczenie do potrzebnego zakresu, redakcję, obserwację lub udział niezależnego audytora, a nie całkowitą odmowę weryfikacji. DPA nie udziela samodzielnego prawa do pobrania kodu źródłowego, danych innych Organizacji ani nieuzgodnionego ingerencyjnego testu bezpieczeństwa; QA10 zapewnia inną skuteczną metodę wykazania zgodności, gdy ich ujawnienie lub taki test nie są potrzebne. Uzgodnienia poufności nie mogą wyłączać ustawowych praw, zgłoszenia naruszeń ani współpracy z organem.
3. **Nie obowiązuje limit jednej kontroli w roku ani bezwzględny termin uprzedzenia.** Incydent, uzasadnione podejrzenie naruszenia, żądanie organu lub nieskuteczność informacji zdalnych mogą uzasadniać kontrolę dodatkową lub pilną. QA10 zapewnia w

dalszym łańcuchu możliwość wykazania zgodności odpowiednią do art. 28 ust. 4 RODO. Jeżeli jej zdaniem instrukcja dotycząca kontroli narusza przepisy ochrony danych, niezwłocznie informuje Klienta zgodnie z §2 ust. 3, nie zastępując tego ogólną odmową audytu.

4. Każda strona ponosi własne koszty udziału w zwykłej kontroli, w tym Klient koszty wybranego przez siebie audytora. Ewentualne dodatkowe, uzasadnione koszty organizacyjne QA10 wymagają uprzedniego wskazania zakresu i sposobu rozliczenia oraz skutecznego uzgodnienia z Klientem; niniejsza DPA nie ustanawia stawki ani automatycznej opłaty za audyt. Koszty nie mogą czynić prawa z art. 28 ust. 3 lit. h RODO iluzorycznym. Brak uzgodnienia lub przedpłaty nie uprawnia do wstrzymania informacji niezbędnych do wykazania zgodności, potrzebnej pilnej kontroli ani wykonania obowiązku ustawowego. QA10 nie obciąża Klienta kosztami naprawy własnych uchybień lub uchybień dalszego procesora ani dodatkowymi kosztami weryfikacji koniecznej wskutek takich uchybień, w zakresie, w jakim są im przypisane. Prawa konsumenta i chronionej JDG oraz bezwzględnie obowiązujące przepisy mają pierwszeństwo.

§9. Zwrot, usunięcie i zmiana dostawcy

1. Po zakończeniu świadczenia czynności przetwarzania QA10, **według wyboru Klienta**, zwraca mu wszystkie dane powierzone w powszechnie używanym formacie albo je usuwa, a także usuwa istniejące kopie, chyba że prawo Unii lub państwa członkowskiego wymaga przechowywania. Klient może przekazać wybór na **hello@qa10.io** lub uzgodnionym kanałem w każdym czasie do końca właściwego okna eksportu; QA10 potwierdza jego otrzymanie. Brak odpowiedzi w ciągu 14 dni nie oznacza rezygnacji z wyboru. QA10 prosi o dyspozycję i zapewnia możliwość zwrotu przez całe właściwe okno. Jeżeli mimo przypomnienia Klient nie wybierze, po upływie okna QA10 stosuje wariant usunięcia, dokumentując wezwanie, termin, zakres i wyjątki prawne. Nie usuwa wcześniej danych potrzebnych do dostępnego zwrotu. Wyrażne żądanie wcześniejszego usunięcia rozpatruje w granicach prawa, praw innych osób i właściwie ustalonego zakresu instrukcji; harmonogram nie uzasadnia przechowywania danych, które zgodnie z prawem powinny być usunięte wcześniej.
2. Harmonogram umowy obejmuje **30 dni po zakończeniu całej Usługi** na dostęp tylko do odczytu i eksportu albo uzgodniony bezpieczny zwrot, następnie **do 30 dni na usunięcie z systemów produkcyjnych**, a następnie **do kolejnych 30 dni na usunięcie lub wygaśnięcie kopii zapasowych**, z pierwszeństwem ust. 3 i wyjątków ustawowych. Samo zakończenie abonamentu nie kończy całej Usługi, jeżeli trwa uprawnienie do korzystania z zakupionych bezterminowych Dodatków na zasadach Regulaminu. Dane pozostające w kopiach są odizolowane od zwykłego użytku i nie służą dalszemu świadczeniu; po odtworzeniu QA10 ponownie stosuje dyspozycję usunięcia. QA10 utrzuła wykonanie i na wniosek przekazuje potwierdzenie oraz informacje o wyjątkach.
3. W zakresie, w jakim Usługa podlega rozporządzeniu (UE) 2023/2854 (**Data Act**), prawo zmiany dostawcy i warunki z § 15 Regulaminu mają pierwszeństwo przed harmonogramem, który skracałby ustawowe uprawnienia. Okres przejściowy trwa

zasadniczo nie dłużej niż **30 dni kalendarzowych** po właściwym okresie wypowiedzenia, nie dłuższym niż **dwa miesiące**, z ustawowymi wyjątkami i prawem Klienta do przedłużenia na zasadach art. 25. **Po zakończeniu okresu przejściowego Klient ma co najmniej 30 dni na odzyskanie danych**, zgodnie z art. 25 ust. 2 lit. g. Decydujące jest późniejsze z przysługujących okien odzyskania. W przypadku pomyślnie ukończonej zmiany dostawcy całkowite usunięcie danych i aktywów następuje po okresie odzyskania albo po upływie późniejszego okresu skutecznie uzgodnionego zgodnie z art. 25 ust. 2 lit. h Data Act. Etapy usunięcia z produkcji i kopii z ust. 2 stosuje się jako taki późniejszy okres tylko w granicach prawa i skutecznego uzgodnienia; nie ograniczają one wyboru Klienta z ust. 1 ani obowiązków RODO. Jeżeli zmiana dostawcy nie została pomyślnie ukończona, sam upływ planowanego okna nie stanowi podstawy pozbawienia Klienta należnego odzyskania danych. Harmonogram z ust. 2 nie daje prawa do opóźnienia usunięcia sprzecznego z Data Act lub RODO. Zakres danych eksportowalnych, aktywów cyfrowych, metadanych i dopuszczalnych wyłączeń określają Regulamin i prawo. DPA nie zmniejsza tego zakresu ani nie gwarantuje identycznego działania u innego dostawcy.

4. Obowiązkowe przechowywanie danych powierzonych po zakończeniu wymaga wskazania właściwej normy, ograniczenia zakresu i okresu oraz odizolowania od zwykłego użytku; QA10 informuje Klienta, o ile prawo tego nie zabrania. Dane rozliczeniowe przetwarzane przez QA10 jako odrębnego administratora na podstawie przepisów rachunkowych lub podatkowych nie są automatycznie kopiami danych powierzonych. Ogólna potrzeba obrony roszczeń nie zezwala na bezterminowe zachowanie całej Organizacji lub dokumentów na podstawie DPA. Żaden wyjątek nie uprawnia do używania danych dla innych klientów lub treningu.
5. Eksport wybranego dokumentu lub techniczny eksport konta nie zastępują pełnego zwrotu danych powierzonych ani zmiany dostawcy. Jeżeli interfejs nie zapewnia potrzebnego zakresu lub formatu, Klient kieruje żądanie na **hello@qa10.io**, a QA10 zapewnia inną bezpieczną drogę realizacji obowiązku. Ograniczenie konkretnego eksportera nie zwalnia z pełnego zwrotu wymaganego DPA i prawem. Usunięcie konta pojedynczego Użytkownika nie oznacza samo w sobie zakończenia Usługi Organizacji, usunięcia wszystkich jej dokumentów i kopii ani rezygnacji z odrębnego newslettera. Zakres takich operacji ustala się osobno z uwzględnieniem instrukcji Klienta i praw osób; pseudonimizacja nie jest automatycznie pełnym usunięciem lub anonimizacją.

§10. Odpowiedzialność, czas i pierwszeństwo

1. DPA obowiązuje od skutecznego zawarcia na czas przetwarzania powierzonych danych, niezależnie od uruchomienia AI. Warunki §5 dotyczą dopuszczenia danych do konkretnej operacji i nie odraczają obowiązywania Regulaminu, Licencji ani pozostałych postanowień DPA. Obowiązki poufności, bezpieczeństwa, pomocy, wykazania zgodności i audytu, zwrotu oraz usunięcia trwają po zakończeniu umowy głównej w zakresie koniecznym do ich wykonania. Zakończenie lub zawieszenie funkcji nie

upoważnia do dalszego używania danych poza niezbędnym zabezpieczeniem, zwrotem, usunięciem i czynnościami wymaganymi prawem.

2. Odpowiedzialność stron określają prawo i **§ 16 Regulaminu, wraz ze wszystkimi przewidzianymi tam wyjątkami**, w szczególności dotyczącymi naruszenia poufności przez QA10. W prawnie dopuszczalnej relacji z przedsiębiorcą zawierającym umowę o charakterze zawodowym stosuje się **jeden wspólny limit dla Usługi, Regulaminu, Licencji i DPA**, bez drugiej puli lub sumowania. DPA nie ustanawia dodatkowych kwot, kar ani odrębnego limitu; § 17 Regulaminu nie stosuje się do konsumentów i chronionych JDG. Żadne odesłanie nie ogranicza praw osób z art. 82 RODO, kompetencji organów, pełnej odpowiedzialności QA10 za wykonanie obowiązków dalszego procesora z art. 28 ust. 4 RODO, odpowiedzialności za szkodę umyślną ani innych roszczeń i obowiązków, których ograniczyć nie wolno. Limit i wyłączenia nie stosują się także do czynów wynikających z rażącego niedbalstwa w takim zakresie, w jakim ograniczenie byłoby niewiążące na podstawie art. 13 rozporządzenia (UE) 2023/2854; nie ograniczają środków ochrony prawnej dotyczących danych, których wyłączyć nie można na podstawie tego przepisu. Nie jest to ogólne wyłączenie limitu dla wszystkich stosunków między przedsiębiorcami. DPA ma pierwszeństwo w zakresie danych powierzonych, z zachowaniem bezwzględnie obowiązujących przepisów i ustawowych praw Data Act; nie tworzy wyjątku od wspólnego limitu poza tymi, które wynikają z prawa i § 16 Regulaminu.
3. Stosuje się prawo polskie. Spory rozstrzyga się zgodnie z Regulaminem i właściwymi przepisami o sądzie, bez ograniczania ustawowej ochrony konsumentów i chronionych JDG oraz kompetencji organu nadzorczego. Nieważność postanowienia nie pozbawia pozostałych skuteczności, o ile mogą obowiązywać samodzielnie; nie zastępuje się nieważnego postanowienia jednostronnym warunkiem o tym samym bezprawnym skutku.
4. Zawieszenie i rozwiązanie umowy głównej podlegają Regulaminowi i prawu. Istotne usuwalne naruszenie obowiązków powierzenia wymaga wezwania do usunięcia na zasadach § 19 Regulaminu, z terminem **14 dni**; pilne zagrożenie, bezprawna instrukcja lub wiążący obowiązek mogą wymagać niezwłocznego, proporcjonalnego wstrzymania danej operacji albo rozwiązania w granicach prawa. Strony współpracują przy ograniczeniu skutków i zapewnieniu legalnego zwrotu lub usunięcia. Zakończenie nie znosi obowiązków z §9, praw ustawowych, należnych rozliczeń ani odpowiedzialności za wcześniejsze zdarzenia i nie stanowi obietnicy dodatkowego dobrowolnego zwrotu opłat.
5. Zmiana DPA wymaga procedury skutecznego związania stron, właściwej formy i reprezentacji oraz odpowiedniego udokumentowania. W stosunku ciągłym stosuje się także § 21 Regulaminu, w tym **30-dniowe uprzedzenie** o proponowanej zmianie na zasadach tego paragrafu. Odrębna procedura zmian dalszych procesorów z §4 nie zastępuje zgody wymaganej dla innych zmian. Wersja 2.1 opublikowana 05.10.2026 ma zastosowanie do nowych umów, dla których została skutecznie udostępniona przed zawarciem i przyjęta zgodnie z §1 ust. 3. Sama publikacja nie zmienia istniejących umów

ani instrukcji, nie działa wstecz i nie usuwa skutków wcześniejszych naruszeń. Milczenie nie zastępuje zgody lub upoważnienia wymaganych prawem.

Załącznik 1: opis powierzenia (art. 28 ust. 3 RODO)

1. Powiązanie z konkretną umową

Powierzenie obejmuje wyłącznie uzgodniony zakres funkcji, danych i osób. Przed powierzeniem strony utrwalają w zamówieniu lub przyjętym uzupełnieniu tego załącznika: tożsamość i rolę Klienta, umocowanie do dalszego powierzenia, jeżeli jest potrzebne, identyfikację umowy i Organizacji, wybrane funkcje, rzeczywiste kategorie danych i osób, czas przetwarzania oraz kontakt do instrukcji i bezpieczeństwa. Wskazują również ograniczenia, integracje i ewentualne odrębnie uzgodnione przetwarzanie danych z art. 9 lub 10 RODO. Treść uzupełnienia musi być dostępna stronom do zachowania. Niewypełnionego zakresu nie domniemywa się z samego wgrania pliku.

2. Przedmiot, czas, charakter, cele, osoby i dane

Element	Zakres umowny
Przedmiot	Obsługa wyodrębnionej przestrzeni danych Klienta w BudOS: przyjmowanie i przechowywanie jego dokumentów i pól, wyszukiwanie i analiza, przygotowanie kosztorysów i projektów ofert, praca uprawnionych Użytkowników, eksport, zwrot i usunięcie. W zakresie funkcji skutecznie zamówionych i wybranych przez Klienta może obejmować bazę wiedzy firmy, dokumenty i kwalifikacje personelu, relacje z kontrahentami i zamawiającymi, kontrakty, historię realizacji, ocenę skuteczności i informacje o konkurencji, a także uzgodnione integracje. Dostępność funkcji zależy od Planu, a dopuszczenie danych do jej użycia wymaga spełnienia warunków DPA.
Czas	Okres skutecznego świadczenia czynności przetwarzania i właściwe okresy zwrotu oraz usunięcia z §9, z pierwszeństwem ustawowego okna odzyskania i ograniczonymi wyjątkami prawnymi. Sam koniec abonamentu przy trwającej Usłudze nie rozpoczyna kasowania.
Charakter czynności	Przyjęcie, zapis, porządkowanie, odczyt, indeksowanie i wyszukiwanie, ekstrakcja tekstu lub rozpoznawanie znaków, wyświetlanie, porównanie, analiza automatyczna, jeżeli została zatwierdzona, przesłanie do upoważnionego operatora, tworzenie i przechowywanie wyniku, kopie, niezbędne wsparcie, wykonanie uzgodnionej integracji, eksport, zwrot i usunięcie. Każda operacja pozostaje w granicach udokumentowanej instrukcji i zatwierdzonych odbiorców.
Cele	Wyłącznie wykonanie funkcji Usługi wybranych i poleconych przez Klienta, w tym pracy nad postępowaniami, kosztorysem, ofertą, wiedzą firmy i realizacją kontraktów, oraz zabezpieczenie i zakończenie tych czynności. Bez marketingu na danych powierzonych, treningu, niezależnej eksploatacji treści Klienta i analityki łączącej dane różnych klientów.

Element	Zakres umowny
Kategorie osób	Pracownicy, współpracownicy i reprezentanci Klienta; osoby kontaktowe wykonawców, podwykonawców, zamawiających i kontrahentów; osoby wymienione w SWZ, ofertach, umowach, załącznikach i zaświadczeniach; osoby fizyczne prowadzące działalność; inne osoby objęte zgodnym z prawem, konkretnie uzgodnionym zakresem.
Zwykłe dane osobowe	Imię, nazwisko, służbowe dane kontaktowe i role, identyfikatory, podpisy, doświadczenie, kwalifikacje, uprawnienia, dane działalności osoby fizycznej, treść ofert, SWZ, umów i korespondencji Klienta, informacje o realizacjach i relacjach z kontrahentami, historia działań w Organizacji oraz dane wynikowe. Identyfikatory krajowe, dane rachunków lub dane prywatnego kontaktu mogą być przyjęte tylko w zakresie niezbędnym do uzgodnionego celu, z odpowiednią ochroną. Wyliczenie nie jest pozwoleniem na zbieranie nadmiarowych danych.
Szczególne kategorie z art. 9 RODO	Przyjmowanie danych o zdrowiu, niepełnosprawności i innych szczególnych kategorii jest ograniczone. Klient powinien usunąć lub zredagować je przed przesłaniem. Wyjątek wymaga uprzedniego uzgodnienia konkretnego zakresu, wykazania niezbędności i podstawy z art. 9 ust. 2 oraz odpowiednich środków bezpieczeństwa. QA10 nie musi przyjmować danych poza uzgodnionym zakresem lub bez wymaganej ochrony. Przypadkowe otrzymanie nie wyłącza RODO: po wykryciu QA10 ogranicza dostęp i dalsze przekazywanie, zawiadamia Klienta oraz postępuje według zgodnej z prawem instrukcji, bez automatycznego zniszczenia z pominięciem obowiązków dowodowych i praw Klienta.
Dane z art. 10 RODO	Przyjmowanie zaświadczeń i informacji KRK oraz danych o wyrokach skazujących, czynach zabronionych i związanych środkach bezpieczeństwa jest ograniczone. Klient powinien usunąć lub zredagować je przed przesłaniem. Wyjątek wymaga uprzedniego uzgodnienia zakresu, wykazania niezbędności oraz przesłanek art. 10, w tym kontroli władz publicznych albo właściwego umocowania w prawie Unii lub państwa członkowskiego z odpowiednimi zabezpieczeniami. Publiczne źródło nie zastępuje tej podstawy. QA10 ogranicza dostęp i przekazywanie, w szczególności do AI; bez wymaganych warunków wstrzymuje operację i zwraca się o legalną instrukcję. Przypadkowe otrzymanie nie wyłącza obowiązków procesora.
Obowiązki i uprawnienia Klienta	Ustalenie celów, podstaw, zakresu i potrzebnych okresów, minimalizacja, informowanie osób, uprawnienia do powierzenia i instrukcji; wybór zwrotu lub usunięcia, otrzymywanie informacji i pomocy, upoważnianie dalszych procesorów i sprzeciw wobec zmian, audyt i inspekcja oraz współpraca w obsłudze praw osób i naruszeń. Szczegóły określają §2, §4 i §6–9.

3. Granice zakresu

1. Samodzielne pozyskiwanie i opracowywanie przez QA10 publicznych źródeł dla własnej bazy, zestawień lub newslettera nie jest powierzeniem konkretnego Klienta tylko dlatego, że korzysta on z tych opracowań. DPA obejmuje operacje wykonywane na jego instrukcję, np. analizę dokumentu w jego Organizacji. Informacje o własnych operacjach QA10 znajdują się w Polityce prywatności.

2. Przygotowanie lub „publikacja” paczki dokumentów w warsztacie ofertowym nie jest samo w sobie publicznym udostępnieniem danych ani złożeniem oferty do zamawiającego. Przekazanie wyników poza Organizację wymaga właściwego działania uprawnionego Użytkownika i podstawy prawnej. Dostęp do integracji zależy od zamówienia i odrębnego podłączenia przez Użytkownika; podłączenie nie zastępuje wymaganych umów i upoważnień dla odbiorców działających w łańcuchu QA10.
3. Przetwarzanie danych powierzonych przez AI, pomoc lub wsparcie pozostaje objęte §3–5 niezależnie od nazwy funkcji. Oprogramowanie do rozpoznawania tekstu, lokalnych modeli, bazy danych lub kolejkowania nie stanowi samo w sobie odrębnego dalszego procesora; przekazanie dokumentu zewnętrznemu operatorowi takiej usługi wymaga uprzedniej kwalifikacji i upoważnienia.

Załącznik 2: mechanizm imiennej autoryzacji dalszych procesorów

1. Warunek przed powierzeniem

Upoważnienie dalszych procesorów wymaga zatwierdzenia konkretnego imiennego wykazu. Wymienienie technologii, modelu lub marki w DPA nie upoważnia żadnego odbiorcy, w tym OpenRouter ani operatorów odrębnego toru pomocy AI. Przed pierwszym powierzeniem QA10 przekazuje Klientowi konkretny, kompletny wykaz odnoszący się do uzgodnionej Organizacji i funkcji, a strony skutecznie ustalają i utrwalają jego treść oraz rodzaj upoważnienia. Jeżeli nie angażuje się odrębnych dalszych procesorów, strony muszą wyraźnie ustalić i udokumentować również taki stan; nie wynika on z pustej tabeli lub braku wpisów.

2. Obowiązkowa treść konkretnego wykazu

Zakres uzupełnienia	Wymagana treść przed przekazaniem danych
Powiązanie i wersja	Oznaczenie Klienta, jego umowy i Organizacji, numer lub inne jednoznaczne oznaczenie wersji wykazu, data obowiązywania oraz zakres funkcji.
Tożsamość i rola	Pełna nazwa prawnego podmiotu, dane pozwalające go zidentyfikować, rola w konkretnym łańcuchu i relacja do QA10 lub wcześniejszego procesora. Sama nazwa oprogramowania, modelu albo hosta nie wystarcza.
Funkcja i dane	Cel zleconej czynności, jej charakter, kategorie osób i danych, dostęp do treści albo tylko określonych metadanych oraz ograniczenia dostępu.
Lokalizacja i dostęp	Rzeczywiste państwa i odpowiednie regiony przetwarzania, przechowywania, kopii i dostępu wsparcia. Gdy konfiguracja pozwala na różne lokalizacje, wskazuje się zatwierdzony zakres, a nie domyślnie cały świat lub sam region serwera.

Zakres uzupełnienia	Wymagana treść przed przekazaniem danych
Transfery	Dla każdej właściwej ścieżki mechanizm rozdziału V RODO, objęci nim importerzy i zakres, skuteczne związanie odpowiednimi zabezpieczeniami, wymagane oceny i środki dodatkowe oraz sposób uzyskania informacji lub kopii.
Umowa i ochrona	Potwierdzenie skutecznego nałożenia obowiązków art. 28 ust. 4 RODO, zakres bezpieczeństwa, pomocy, kontroli, retencji i zwrotu lub usunięcia. Nie zastępuje się tego linkiem do nieprzyjętych warunków.
Szczegóły AI, jeśli dotyczy	Oddzielna identyfikacja bramki i rzeczywistych operatorów endpointów, zatwierdzone funkcje i modele, zakres zakazu treningu i ZDR, odrębne metadane, narzędzia i przechowywanie, dopuszczalne trasy zastępcze lub ich brak oraz spełnienie warunku zatrzymania niezgodnej operacji.
Upoważnienie	Wybór upoważnienia szczególnego albo ogólnego, jego zakres i ograniczenia, sposób oraz czas skutecznego udzielenia przez umocowaną osobę; przy upoważnieniu ogólnym uzgodniony kanał zawiadomień i procedura §4 ust. 3.

3. Stosowanie i zmiany

1. QA10 zachowuje dowód skutecznego udostępnienia i zatwierdzenia konkretnego wykazu, upoważnienia oraz związania podmiotów w łańcuchu **przed pierwszym przekazaniem**. Bez właściwego upoważnienia nie przekazuje danych danemu podmiotowi na podstawie DPA. Upoważnienie nie zastępuje oceny bezpieczeństwa ani legalności transferu.
2. Wykaz obejmuje rzeczywistych odrębnych odbiorców wykonujących czynności powierzenia, w tym, zależnie od uzgodnionego zakresu, hosting, przechowywanie i kopie, pocztę, wsparcie oraz inferencję. Nie obejmuje automatycznie wszystkich narzędzi własnego marketingu QA10, płatności lub własnej infrastruktury. Role rozstrzyga się dla konkretnej operacji. PostgreSQL, Redis, Postal, biblioteka OCR lub lokalny model są nazwami oprogramowania, nie samodzielną identyfikacją procesora.
3. Zmiany objęte upoważnieniem ogólnym podlegają aktywnemu zawiadomieniu **14 dni kalendarzowych przed zmianą** i prawu sprzeciwu z §4 ust. 3. Zmiany poza jego zakresem wymagają nowego właściwego upoważnienia. Historia wykazu, sprzeciwów i rozstrzygnięć pozostaje dostępna w zakresie potrzebnym do wykazania zgodności.

Załącznik 3: wymagane środki techniczne i organizacyjne (TOM)

1. Dobór i zapewnienie środków

Poniższe środki są minimalnymi wymaganiami dla powierzenia, dobieranymi i uszczegóławianymi do ryzyka rzeczywistego zakresu. QA10 musi zapewnić i udokumentować środki odpowiednie do uzgodnionych danych przed ich przyjęciem, przekazać Klientowi ich opis i utrzymywać je podczas przetwarzania. Dane można powierzyć dopiero po zapewnieniu środków właściwych dla uzgodnionego zakresu. QA10 wskazuje Klientowi zastosowane środki, ich zakres i istotne ograniczenia oraz udostępnia

dokumentację pozwalającą wykazać skuteczność, bez niepotrzebnego ujawniania szczegółów podatnych na nadużycie.

2. Pełny zakres wymaganych kontroli

Obszar	Wymagane środki i sposób wykazania
Zarządzanie ochroną i ryzykiem	Ustalenie odpowiedzialności za ochronę danych, opis czynności i przepływów, inwentarz danych, systemów, lokalizacji i kopii, ocena zagrożeń utraty, zmiany, ujawnienia i nieuprawnionego dostępu. Dokumentowanie doboru ochrony z uwzględnieniem art. 32 oraz podwyższonego ryzyka danych z art. 9 lub 10 i ocen skutków.
Personel i poufność	Udokumentowane upoważnienia ograniczone do zadań, zobowiązania lub ustawowy obowiązek poufności, odpowiednie szkolenia, kontrola instrukcji, nadawanie i odbieranie dostępu przy zmianie roli lub zakończeniu współpracy.
Tożsamość i dostęp	Zasada najmniejszych uprawnień, imienne uprawnienia, odpowiednie uwierzytelnianie i ochrona kont administracyjnych, przeglądy dostępu, kontrola sesji i tokenów oraz ograniczenie i dokumentowanie dostępu wsparcia. Ochrona hasła, kluczy i innych poświadczeń przed ujawnieniem i nieuprawnionym użyciem.
Rozdzielenie Organizacji	Logiczne oddzielenie danych i uprawnień klientów w aplikacji, API, bazie, przechowywaniu, wyszukiwaniu, eksporcie i kopiach. Sprawdzanie autoryzacji dla konkretnego obiektu, nie wyłącznie identyfikatora podanego przez Użytkownika; testy dostępu pomiędzy Organizacjami.
Transmisja	Ochrona kanałów użytkownika, API, administracji, poczty i zewnętrznych usług odpowiednia do danych i ryzyka, w tym właściwa konfiguracja szyfrowania transmisji i weryfikacja odbiorcy. Udokumentowany zakres ochrony połączeń wewnętrznych i zewnętrznych; każdy kanał wymaga ochrony odpowiedniej do danych i ryzyka.
Przechowywanie, szyfrowanie i pseudonimizacja	Ochrona baz, plików, indeksów, logów i kopii przed nieuprawnionym odczytem i zmianą. Szyfrowanie i pseudonimizacja w zakresie odpowiednim do ryzyka, ochrona i zarządzanie kluczami, oddzielenie danych identyfikacyjnych, gdy jest właściwe. Dokumentacja wskazuje rzeczywisty zakres, ograniczenia i kontrolę dostępu; nie zakłada anonimizacji z samego skrótu lub pseudonimu.
Minimalizacja i logowanie	Ograniczenie danych do potrzeb funkcji, ograniczenie treści w diagnostyce i zgłoszeniach, ochrona logów i śladów dostępu przed zmianą i nieuprawnionym ujawnieniem. Ustalenie zakresu i okresów logowania, kontrola redakcji danych oraz oddzielenie niezbędnych metadanych od dokumentów, promptów i wyników. Brak wykorzystywania powierzonych treści w niezatwierdzonej analityce.
AI i kontrola odbiorców	Udokumentowanie bramki, operatora, endpointu, funkcji, regionu, umowy i upoważnienia dla każdej ścieżki. Minimalizacja promptu, zakaz treningu, weryfikacja zakresu ZDR i odrębnych metadanych, wykluczenie niezatwierdzonych narzędzi, wtyczek, plików i tras zastępczych. Sprawdzenie zatrzymania operacji, gdy nie ma zgodnej ścieżki, także dla odmiennych trybów wywołania. Każdy odbiorca wymaga upoważnienia prawnego niezależnie od preferencji technicznej lub listy dozwolonych hostów.

Obszar	Wymagane środki i sposób wykazania
Środowiska i zmiany	Oddzielenie produkcji i środowisk testowych bez kopiowania danych powierzonych do testów, kontrola zmian konfiguracji i wdrożeń, zarządzanie podatnościami i aktualizacjami, sprawdzenie wpływu istotnej zmiany na bezpieczeństwo, retencję i odbiorców przed dopuszczeniem operacji.
Ciągłość, odporność i odtworzenie	Środki zapewniające trwałą poufność, integralność, dostępność i odporność systemów. Kontrolowane kopie, odpowiednia ochrona lokalizacji i nośników, dokumentacja odtwarzania i zdolność przywrócenia dostępności oraz dostępu w odpowiednim czasie po incydencie fizycznym lub technicznym. Testy odtworzenia odpowiednie do ryzyka; bez dodatkowego liczbowego SLA.
Incydenty	Wykrywanie i rejestrowanie zdarzeń, ocena naruszenia, przypisanie odpowiedzialności, zapewnienie kontaktu i zawiadomienia Klienta bez zbędnej zwłoki, najpóźniej w 24 godziny od stwierdzenia, współpraca przy ograniczeniu skutków i dokumentacja etapowych informacji z §7. Procedura obejmuje informacje od dalszych procesorów.
Prawa osób i pomoc	Możliwość odnalezienia danych w uzgodnionym zakresie, obsługa instrukcji i pomoc w realizacji art. 12–22 oraz art. 32–36 RODO, proporcjonalna weryfikacja osoby umocowanej, bezpieczne przekazywanie informacji i prowadzenie dokumentacji żądań. Częściowy eksport konta nie zamyka pełnego wniosku.
Eksport, zwrot i retencja	Inwentarz danych powierzonych, metadanych i kopii, ustalenie początku i końca właściwego okna odzyskania, zapewnienie pełnego zwrotu inną bezpieczną drogą, jeżeli interfejs nie wystarcza. Udokumentowane wykonanie 30 dni odzyskania, do 30 dni usunięcia produkcji i do kolejnych 30 dni usunięcia lub wygaśnięcia kopii z §9, z pierwszeństwem Data Act, wyboru Klienta i wyjątków ustawowych.
Usuwanie i kopie	Kontrola rzeczywistego usunięcia lub nieodwracalnego wygaśnięcia kopii, odizolowanie danych oczekujących na wygaśnięcie, ponowne zastosowanie dyspozycji po odtworzeniu, ograniczenie i dokumentowanie prawnie wymaganego zatrzymania. Potwierdzenie wykonania nie opiera się wyłącznie na dezaktywacji konta.
Dalszy łańcuch i transfery	Weryfikacja tożsamości prawnej, skutecznych umów, upoważnień i lokalizacji, przekazanie obowiązków ochrony i kontroli, aktywne zawiadomienia i obsługa sprzeciwu, udokumentowanie podstaw transferów oraz potrzebnych środków dodatkowych. Zmiana operatora technicznego nie obchodzi §4–5.
Testy, ocena i audyt	Regularne testowanie, mierzenie i ocenianie skuteczności środków odpowiednio do ryzyka i zmian, dokumentowanie wyników i działań naprawczych, dostępność informacji dla Klienta i współpraca przy audycie oraz inspekcji z §8. Ocena obejmuje rzeczywisty zakres i skuteczność zastosowanych środków, a nie samą obecność procedury lub narzędzia.

3. Utrzymanie i informacje dla Klienta

1. QA10 dokumentuje zastosowane środki, ich ocenę i istotne zmiany, a także zakres danych produkcyjnych i kopii, wykonanie zwrotu i usunięcia oraz ponowne zastosowanie dyspozycji po odtworzeniu. Klient otrzymuje opis odpowiedni do kategorii danych i ryzyka, w tym danych z art. 9 lub 10 i oceny skutków, bez udostępniania danych innych klientów lub niepotrzebnych sekretów bezpieczeństwa.
2. Równoważna zmiana techniczna jest dopuszczalna, jeżeli nie obniża wymaganego poziomu ochrony i pozostaje zgodna z instrukcjami, DPA oraz zasadami zmian odbiorców i transferów. Istotne obniżenie ochrony podlega §3 ust. 2 i nie może prowadzić do niezgodnego przetwarzania.
3. Brak zapewnienia właściwego środka oznacza konieczność niedopuszczenia lub wstrzymania objętej nim operacji, a nie zwolnienie QA10 z odpowiedzialności albo udzielenie przez Klienta blankietowej zgody na ryzyko. QA10 jest zobowiązana faktycznie wykonywać DPA i przyjęte załączniki przez cały okres przetwarzania.