

Umowa powierzenia przetwarzania danych (DPA)

Ostatnia aktualizacja: 1 maja 2026 r. · Umowa zgodna z art. 28 RODO.

To tłumaczenie ma charakter wyłącznie informacyjny. W razie rozbieżności między tym tłumaczeniem a wersją angielską rozstrzyga wersja angielska.

Jak to działa

Niniejsza umowa powierzenia stanowi część warunków korzystania z usługi. Zaczyna obowiązywać automatycznie, gdy zostanie utworzona przestrzeń robocza i zostaną w niej zapisane dane osobowe. Organizacja klienta, do której należy przestrzeń robocza, jest administratorem; Dazr jest podmiotem przetwarzającym. Podpis nie jest potrzebny; jeśli Twój proces zakupowy wymaga egzemplarza podpisanego przez obie strony, napisz na legal@dazr.eu.

1. Definicje

Pojęcia użyte w niniejszej umowie mają znaczenie nadane im w rozporządzeniu (UE) 2016/679 (RODO). „Dane osobowe klienta” to dane osobowe, które administrator (lub działający w jego imieniu członkowie i audytorzy) umieszcza w przestrzeni roboczej, w tym dane osobowe zawarte w zadaniach kontrolnych, dowodach, komentarzach, plikach, ryzykach, incydentach, kartach dostawców, danych członków i zaproszeniach, zgłoszeniach z publicznego portalu oraz w dzienniku aktywności.

2. Przedmiot, czas trwania, charakter i cel

- Przedmiot: przetwarzanie danych osobowych klienta, aby administrator mógł prowadzić swój program zgodności w zakresie bezpieczeństwa informacji i ochrony danych za pomocą platformy Dazr Compliance.
- Czas trwania: okres subskrypcji administratora, powiększony o okres przejściowy po jej zakończeniu przewidziany w warunkach korzystania z usługi.
- Charakter i cel: hosting, przechowywanie, przesyłanie, pobieranie, usuwanie oraz operacje opisane w warunkach korzystania z usługi i w polityce prywatności.
- Rodzaj danych osobowych: dane identyfikacyjne członków przestrzeni roboczych i zaproszonych audytorów (adres e-mail, imię i nazwisko, rola); w odpowiednich przypadkach dane identyfikacyjne osób zgłaszających przez publiczny portal i osób zgłaszających incydenty; dane kontaktowe pracodawców i metadane operacyjne przesłane przez administratora. Administrator odpowiada za to, by nie przysyłać szczególnych kategorii danych, chyba że pozwala na to jego własna podstawa prawna.
- Kategorie osób, których dane dotyczą: pracownicy, współpracownicy i zaproszeni audytorzy zewnętrzni administratora oraz wszystkie osoby wskazane w treściach dotyczących zgodności, które administrator postanowi przesłać.

3. Obowiązki podmiotu przetwarzającego

1. Przetwarzamy dane osobowe klienta wyłącznie na udokumentowane polecenie administratora. Poleceniem jest korzystanie z przewidzianych funkcji platformy; jeśli uznamy, że polecenie narusza RODO lub inne przepisy Unii lub państwa członkowskiego o ochronie danych, informujemy o tym administratora.
2. Zapewniamy, że osoby upoważnione do przetwarzania danych osobowych klienta zobowiązały się do zachowania poufności.
3. Podejmujemy wszystkie środki wymagane na mocy art. 32 RODO (bezpieczeństwo przetwarzania). Aktualne środki opisuje sekcja 7.
4. Przestrzegamy warunków art. 28 ust. 2 i 4 dotyczących korzystania z usług dalszych podmiotów przetwarzających (zob. sekcja 6).
5. Uwzględniając charakter przetwarzania i dostępne nam informacje, pomagamy administratorowi wywiązać

się z obowiązku odpowiadania na żądania osób, których dane dotyczą, zgłaszania naruszeń, przeprowadzania ocen skutków oraz uprzednich konsultacji z organami nadzorczymi (art. 28 ust. 3 lit. e i f).

6. Po zakończeniu świadczenia usług, zależnie od decyzji administratora, usuwamy lub zwracamy wszystkie dane osobowe klienta oraz usuwamy istniejące kopie, chyba że prawo Unii lub państwa członkowskiego nakazuje ich przechowywanie.
7. Udostępniamy administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków z art. 28 oraz umożliwiamy przeprowadzanie audytów, w tym inspekcji, i przyczyniamy się do nich (zob. sekcja 9).

4. Obowiązki administratora

- Administrator zapewnia, że ma podstawę prawną z art. 6 (a w odpowiednich przypadkach z art. 9) dla danych osobowych, które umieszcza w przestrzeni roboczej.
- Administrator odpowiada za prawdziwość danych osobowych klienta i za odpowiadanie na żądania osób, których dane dotyczą, w odniesieniu do swojej przestrzeni roboczej (otrzymane przez nas żądania przekazujemy administratorowi i pomagamy mu zgodnie z art. 28 ust. 3 lit. e).
- Administrator kontroluje dostęp (role członków, zaproszenia audytorów, publiczny portal zgłoszeń) za pomocą ustawień platformy.

5. Przekazywanie danych do państw trzecich

Dane osobowe klienta są domyślnie przechowywane w Unii Europejskiej. Jeśli dalszy podmiot przetwarzający ma siedzibę poza UE, przekazywanie danych odbywa się na podstawie standardowych klauzul umownych Komisji Europejskiej (decyzja 2021/914), moduł 3 (od podmiotu przetwarzającego do podmiotu przetwarzającego), z dodatkowymi środkami opisanymi w sekcji 7. Aktualną listę dalszych podmiotów przetwarzających i ich lokalizacje podaje strona [/legal/subprocessors](#).

6. Dalsze podmioty przetwarzające

1. Administrator upoważnia nas do korzystania z usług dalszych podmiotów przetwarzających w celu świadczenia usługi. Aktualna lista znajduje się na stronie [/legal/subprocessors](#).
2. O planowanym dodaniu lub zastąpieniu dalszego podmiotu przetwarzającego informujemy administratora z co najmniej 30-dniowym wyprzedzeniem, przez subskrypcję e-mailową na tej stronie lub e-mailem do właściciela przestrzeni roboczej.
3. Administrator może wnieść sprzeciw z uzasadnionych przyczyn związanych z ochroną danych. Jeśli nie możemy go uwzględnić, administrator może wypowiedzieć daną usługę i otrzymać proporcjonalny zwrot za niewykorzystaną część bieżącego okresu rozliczeniowego.
4. Na mocy pisemnej umowy nakładamy na każdy dalszy podmiot przetwarzający obowiązki w zakresie ochrony danych nie mniej rygorystyczne niż te z niniejszej umowy i odpowiadamy wobec administratora za wykonanie obowiązków dalszego podmiotu przetwarzającego.

7. Środki bezpieczeństwa (art. 32)

- Szyfrowanie. Dane osobowe klienta są szyfrowane w spoczynku algorytmem AES-256-GCM na poziomie aplikacji, oprócz szyfrowania stosowanego przez dostawcę przechowywania danych. Cała transmisja odbywa się przez HTTPS z HSTS preload, bez nieszyfrowanej alternatywy. Klucze są wyprowadzane przez HKDF z klucza głównego przechowywanego wyłącznie w zmiennych środowiskowych infrastruktury produkcyjnej.
- Kontrola dostępu. Kontrola dostępu oparta na rolach w platformie (właściciel, administrator, członek, audytor); ograniczone w czasie i odwoływalne sesje audytorów. Dostęp operacyjny ma tylko niewielki zespół wsparcia przez portal wsparcia, który z założenia pokazuje wyłącznie metadane.
- Uwierzytelnianie. Logowanie bez hasła za pomocą jednorazowego kodu. Tokeny sesji podpisane HMAC o ograniczonej ważności. Limity zapytań na każdym publicznym punkcie dostępu, także przy logowaniu

administracyjnym.

- Odporność i integralność. Dziennik aktywności w trybie tylko do dopisywania, obejmujący każdą operację zmieniającą stan. Kopie zapasowe w UE. Integralność przechowywanych danych jest weryfikowana znacznikami uwierzytelniającymi AEAD; zmieniony szyfrogram powoduje błąd i nie jest udostępniany.
- Sieć i nagłówki. Ścisła polityka Content-Security-Policy z listą dozwolonych skryptów wbudowanych identyfikowanych skrótem, ścisłe X-Frame-Options, X-Content-Type-Options nosniff i HSTS preload.
- Zarządzanie podatnościami. Zależności mają przypięte wersje; śledzimy komunikaty bezpieczeństwa i instalujemy poprawki w terminach odpowiednich do ich wagi.

8. Naruszenie ochrony danych osobowych

Jeśli dowiemy się o naruszeniu ochrony danych osobowych klienta, zawiadomimy właściciela przestrzeni roboczej bez zbędnej zwłoki, nie później niż 72 godziny po stwierdzeniu naruszenia (art. 33 ust. 2). Zawiadomienie opisuje, w zakresie, w jakim są znane: charakter naruszenia, jego prawdopodobne konsekwencje, podjęte lub proponowane środki oraz punkt kontaktowy, w którym można uzyskać więcej informacji. Pomagamy administratorowi w wypełnieniu jego własnych obowiązków zgłoszeniowych z art. 33 i 34.

9. Audyty

Administrator (lub upoważniony przez niego audytor zewnętrzny) może sprawdzić przestrzeganie niniejszej umowy raz na dwanaście miesięcy, po pisemnym zawiadomieniu z co najmniej 30-dniowym wyprzedzeniem, w godzinach pracy, w sposób, który nie zakłóca nadmiernie naszej działalności i szanuje poufność danych innych klientów. Za audyty wykraczające poza ten zakres możemy pobrać rozsądną opłatę. Jeśli obowiązek audytu z art. 28 ust. 3 lit. h można spełnić zaświadczeniem niezależnej strony trzeciej, którym dysponujemy, prześlemy je zamiast audytu na miejscu.

10. Odpowiedzialność

Odpowiedzialność każdej ze stron z tytułu niniejszej umowy podlega ograniczeniom określonym w warunkach korzystania z usługi. Ograniczenia te nie dotyczą odpowiedzialności za szkody poniesione przez osoby, których dane dotyczą, na podstawie art. 82 RODO.

11. Okres obowiązywania i rozwiązanie

Niniejsza umowa obowiązuje tak długo, jak przetwarzamy dane osobowe klienta, i pozostaje w mocy po rozwiązaniu warunków korzystania z usługi w zakresie i przez czas, w jakim nadal przechowujemy takie dane. Sekcje 8 (naruszenia), 9 (audyty) i 12 (zwrot i usunięcie) obowiązują także po rozwiązaniu umowy.

12. Zwrot i usunięcie danych

Po zakończeniu usługi administrator może wyeksportować dane przestrzeni roboczej narzędziami eksportu platformy w 30-dniowym okresie przejściowym przewidzianym w warunkach korzystania z usługi. Po tym okresie usuwamy dane osobowe klienta; kopie zapasowe wygasają zgodnie z naszym harmonogramem przechowywania. Dane, które musimy przechowywać (np. faktury zgodnie z włoskim prawem handlowym), przechowujemy tylko przez czas trwania tego obowiązku.

13. Pierwszeństwo dokumentów

W razie sprzeczności między niniejszą umową a warunkami korzystania z usługi lub polityką prywatności w sprawach przetwarzania danych pierwszeństwo ma niniejsza umowa. Standardowe klauzule umowne włączone dla przekazywania danych poza UE mają pierwszeństwo przed niniejszą umową i warunkami korzystania z usługi w sprawach, które regulują.

14. Zawiadomienia

- Do Dazr: privacy@dazr.eu (ochrona danych) lub security@dazr.eu (incydenty).
- Do administratora: adres e-mail właściciela przestrzeni roboczej zapisany w chwili zawiadomienia.