

Umowa powierzenia przetwarzania danych osobowych

Wzór – do zawarcia wraz z umową o świadczenie usługi ApliFlow

zawarta w dniu w pomiędzy:

.....
z siedzibą w, NIP,
reprezentowaną/-ym przez,
zwaną/-ym dalej „Administratorem”,

a

Markiem Czarnowskim, prowadzącym działalność gospodarczą pod firmą **Encode Marek Czarnowski**, Mała Huta 42E, 16-402 Suwałki, NIP 8442256350, REGON 362210145, zwanym dalej „Podmiotem przetwarzającym”,

łącznie zwanymi „Stronami”.

§ 1. Przedmiot umowy

1. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych w imieniu Administratora, na zasadach określonych w niniejszej umowie oraz w art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (dalej: „RODO”).
2. Powierzenie następuje w związku z umową o świadczenie usługi dostępu do systemu ApliFlow z dnia (dalej: „Umowa główna”).

§ 2. Zakres, charakter i cel przetwarzania

1. Celem przetwarzania jest świadczenie Usługi określonej w Umowie głównej, tj. udostępnienie Administratorowi systemu do elektronicznej obsługi naborów wniosków, w tym przyjmowania wniosków, ich oceny, publikowania wyników i obsługi sprawozdań.
2. Charakter przetwarzania: przechowywanie, organizowanie, porządkowanie, przeglądanie, udostępnianie upoważnionym użytkownikom Administratora, eksport, usuwanie oraz tworzenie kopii zapasowych – w systemie informatycznym, w sposób zautomatyzowany.
3. Kategorie osób, których dane dotyczą: wnioskodawcy i osoby ich reprezentujące, osoby wskazane we wnioskach (np. zawodnicy, uczniowie, opiekunowie prawni, członkowie organizacji), eksperci i członkowie komisji oceniających, pracownicy i współpracownicy Administratora korzystający z systemu.
4. Rodzaje danych: dane identyfikacyjne i kontaktowe (np. imię, nazwisko, adres, e-mail, telefon), dane zawarte w treści wniosków, załącznikach i sprawozdaniach – w zakresie określonym przez Administratora w formularzach naboru, dane o ocenach i decyzjach, dane logowania i aktywności użytkowników systemu.
5. Jeżeli Administrator zbiera w systemie dane szczególnych kategorii (art. 9 RODO) lub dane dotyczące wyroków skazujących (art. 10 RODO), informuje o tym Podmiot przetwarzający przed rozpoczęciem naboru.
6. Dane przetwarzane są przez czas obowiązywania Umowy głównej oraz przez okres potrzebny do ich zwrotu lub usunięcia zgodnie z § 8.

§ 3. Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający przetwarza dane wyłącznie na udokumentowane polecenie Administratora. Za udokumentowane polecenie uważa się niniejszą umowę, Umowę główną oraz czynności wykonywane przez Administratora w systemie (konfiguracja naborów, formularzy, ról i uprawnień). Jeżeli polecenie Administratora narusza w ocenie Podmiotu przetwarzającego przepisy o ochronie danych, Podmiot przetwarzający niezwłocznie o tym informuje.
2. Podmiot przetwarzający zapewnia, że osoby upoważnione do przetwarzania danych zobowiązały się do zachowania ich w tajemnicy, także po zakończeniu współpracy.
3. Podmiot przetwarzający stosuje środki techniczne i organizacyjne wymagane na mocy art. 32 RODO, opisane w Załączniku nr 1.
4. Podmiot przetwarzający, w miarę możliwości i uwzględniając charakter przetwarzania, pomaga Administratorowi wywiązać się z obowiązku odpowiadania na żądania osób, których dane dotyczą (art. 12–22 RODO), w szczególności przez funkcje systemu umożliwiające wyszukanie, eksport, poprawienie i usunięcie danych.
5. Podmiot przetwarzający pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO, uwzględniając charakter przetwarzania i dostępne mu informacje.
6. Podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 RODO.

§ 4. Dalsze powierzenie

1. Administrator udziela ogólnej zgody na korzystanie przez Podmiot przetwarzający z usług dalszych podmiotów przetwarzających. Na dzień zawarcia umowy jest nim:
OVH Sp. z o.o. (grupa OVHcloud) – usługi hostingu i infrastruktury serwerowej oraz serwer poczty elektronicznej; centrum danych w Warszawie.
2. Podmiot przetwarzający informuje Administratora o zamiarze dodania lub zastąpienia dalszego podmiotu przetwarzającego z co najmniej 14-dniowym wyprzedzeniem, drogą elektroniczną. Administrator może w tym terminie wyrazić sprzeciw. W razie sprzeciwu Strony uzgodnią rozwiązanie, a w braku porozumienia Administrator może wypowiedzieć Umowę główną ze skutkiem na dzień zmiany.
3. Podmiot przetwarzający nakłada na dalszy podmiot przetwarzający obowiązki ochrony danych nie mniejsze niż określone w niniejszej umowie i odpowiada wobec Administratora za wypełnianie przez niego tych obowiązków.
4. Dane przetwarzane są na terytorium Europejskiego Obszaru Gospodarczego. Przekazanie danych poza EOG wymaga uprzedniej pisemnej zgody Administratora.

§ 5. Naruszenia ochrony danych

1. Podmiot przetwarzający zgłasza Administratorowi stwierdzone naruszenie ochrony danych osobowych bez zbędnej zwłoki, nie później niż w ciągu 36 godzin od jego stwierdzenia, na adres e-mail wskazany w § 9.
2. Zgłoszenie zawiera, w miarę możliwości, informacje wymienione w art. 33 ust. 3 RODO. Informacje, których nie można przekazać od razu, Podmiot przetwarzający przekazuje niezwłocznie, gdy staną się dostępne.
3. Podmiot przetwarzający podejmuje działania w celu ograniczenia skutków naruszenia i współpracuje z Administratorem przy jego obsłudze.

§ 6. Prawo kontroli

1. Podmiot przetwarzający udostępnia Administratorowi informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.
2. Administrator może przeprowadzić audyt lub inspekcję, w tym przez upoważnionego audytora, po uprzedzeniu Podmiotu przetwarzającego z co najmniej 14-dniowym wyprzedzeniem, w dniach i godzinach pracy, nie częściej niż raz w roku – chyba że kontrola jest związana z naruszeniem ochrony danych lub kontrolą organu nadzorczego.
3. W zakresie infrastruktury dalszego podmiotu przetwarzającego Administrator przyjmuje jako potwierdzenie stosowanych środków certyfikaty i raporty udostępniane przez ten podmiot (m.in. ISO/IEC 27001, 27017, 27018, 27701).

§ 7. Odpowiedzialność

Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem danych niezgodnym z niniejszą umową lub RODO, na zasadach określonych w art. 82 RODO.

§ 8. Czas trwania i zakończenie

1. Umowa obowiązuje przez czas obowiązywania Umowy głównej.
2. Przed zakończeniem Umowy głównej Administrator może wyeksportować dane z systemu. Na wniosek Administratora złożony nie później niż w dniu zakończenia Umowy głównej Podmiot przetwarzający przekaze mu dane w formacie elektronicznym (np. XLSX, CSV, PDF i pliki załączników).
3. W ciągu 30 dni od zakończenia Umowy głównej Podmiot przetwarzający usuwa dane Administratora z systemu, a z kopii zapasowych – z upływem cyklu ich rotacji, chyba że przepisy prawa nakazują dalsze przechowywanie. Na żądanie Administratora Podmiot przetwarzający potwierdza usunięcie danych.

§ 9. Postanowienia końcowe

1. Osoby do kontaktu w sprawach ochrony danych:
 - po stronie Administratora:
 - po stronie Podmiotu przetwarzającego: Marek Czarnowski, marek@encode.com.pl, tel. 507 111 750.
2. Zmiany umowy wymagają formy pisemnej lub elektronicznej pod rygorem nieważności.
3. W sprawach nieuregulowanych stosuje się przepisy RODO, ustawy o ochronie danych osobowych oraz Kodeksu cywilnego.
4. W razie sprzeczności między niniejszą umową a Umową główną w zakresie ochrony danych osobowych pierwszeństwo ma niniejsza umowa.
5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron, albo w formie elektronicznej opatrzonej kwalifikowanymi podpisami elektronicznymi.

Administrator

Podmiot przetwarzający

Załącznik nr 1. Środki techniczne i organizacyjne

Obszar	Stosowane środki
Infrastruktura	System działa w centrum danych OVHcloud w Warszawie. Dostawca infrastruktury posiada certyfikaty ISO/IEC 27001, 27017, 27018 i 27701.
Szyfrowanie transmisji	Połączenia z systemem są szyfrowane protokołem HTTPS (TLS).
Uwierzytelnianie	Indywidualne konta użytkowników; hasła przechowywane wyłącznie w postaci skrótu kryptograficznego (bcrypt).
Kontrola dostępu	Role i uprawnienia nadawane przez Administratora; eksperci widzą wyłącznie przydzielone im wnioski; separacja danych poszczególnych klientów.
Kopie zapasowe	Codzienne kopie zapasowe bazy danych i załączników, szyfrowane, przechowywane przez 30 dni poza serwerem produkcyjnym, w infrastrukturze OVHcloud na terenie EOG
Aktualizacje	Regularne aktualizacje bezpieczeństwa systemu operacyjnego, środowiska PHP, frameworka Laravel i zależności.
Dostęp administracyjny	Dostęp do serwerów ma wyłącznie Podmiot przetwarzający, przez szyfrowane połączenie SSH.
Rozliczalność	Rejestrowanie w dzienniku zdarzeń logowań oraz operacji wykonywanych przez użytkowników w systemie.
Organizacja	Pisemne upoważnienia i zobowiązania do zachowania poufności; procedura obsługi naruszeń ochrony danych.

Wzór umowy ma charakter informacyjny i może zostać dostosowany do wymagań Administratora.