



WZÓR_Umowa
powierzenia przetwarzania danych osobowych

zawarta w dniu

pomiędzy:

Wyższą Szkołą Bankową w Warszawie z siedzibą w Warszawie przy ul. Łabiszyńskiej 25, 03-204 Warszawa, NIP 1132187591, REGON 016174673, wpisaną pod pozycją 311 do ewidencji uczelni niepublicznych i związków uczelni niepublicznych, prowadzonej przez Ministra Edukacji i Nauki, zgodnie z przepisami ustawy Prawo o szkolnictwie wyższym i nauce, reprezentowaną przez Kanclerza Karola Cyrulika na podstawie pełnomocnictwa udzielonego przez Rektora Wyższej Szkoły Bankowej w Warszawie Piotra Olafa Żylicza („Administrator”)

a

..... („Przetwarzający”),

dalej łącznie zwanymi jako „Strony”.

Mając na uwadze, że:

1. Strony zawarły umowę w sprawie *dostawy i wdrożenia systemu Elektronicznego Obiegu Dokumentów (EOD) w WSB Warszawa („Umowa Podstawowa”)*, w związku z wykonywaniem której Administrator powierza Przetwarzającemu przetwarzanie danych osobowych w zakresie określonym niniejszą Umową powierzenia przetwarzania danych osobowych („Umowa”);
2. Celem Umowy jest ustalenie warunków, na jakich Przetwarzający wykonuje operacje przetwarzania Danych Osobowych w imieniu Administratora;
3. Strony zawierając Umowę dążą do takiego uregulowania zasad przetwarzania Danych Osobowych, aby odpowiadały one w pełni postanowieniom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej **RODO**,

Strony postanowiły zawrzeć Umowę o następującej treści:

1. Opis Przetwarzania

- 1.1. **Przedmiot [art. 28 ust. 3 RODO]** Na warunkach określonych niniejszą Umową oraz Umową Podstawową, Administrator powierza Przetwarzającemu przetwarzanie (w rozumieniu RODO) dalej opisanych Danych Osobowych.
- 1.2. **Czas [art. 28 ust. 3 RODO]** Przetwarzanie będzie wykonywane w okresie obowiązywania Umowy Podstawowej.
- 1.3. **Charakter i cel [art. 28 ust. 3 RODO]** Powierzenie przetwarzania danych osobowych następuje wyłącznie w celu wykonania Umowy Podstawowej.
- 1.4. **Rodzaj danych [art. 28 ust. 3 RODO]** Przetwarzanie obejmować będzie następujące rodzaje danych osobowych („Dane”):

Dane zwykłe:

1. imię i nazwisko,
2. numer ewidencyjny PESEL, NIP, REGON
3. adres e-mail,
4. numery telefonów,
5. adres korespondencyjny,

1.5 Kategorie osób [art. 28 ust. 3 RODO] Dane określone w pkt 1.4 dotyczą następujących kategorii osób:

1. pracownicy Administratora i podmiotów stowarzyszonych Administratora,
2. klienci usług Administratora i podmiotów stowarzyszonych Administratora.

2. Podpowierzenie

- 2.1. **Podpowierzenie [art. 28 ust. 2 RODO]** Przetwarzający może powierzyć konkretne operacje przetwarzania Danych („podpowierzenie”) w drodze pisemnej umowy podpowierzenia („**Umowa Podpowierzenia**”) innym podmiotom przetwarzającym („**Podprzetwarzający**”), pod warunkiem uprzedniej pisemnej akceptacji Podprzetwarzającego przez Administratora.
- 2.2. W przypadku podpowierzenia przetwarzania danych osobowych, Przetwarzający zobowiązany jest do zawarcia umowy z Podprzetwarzającym na co najmniej takich samych warunkach, jakie na mocy niniejszej Umowy nałożone są na Przetwarzającego. Umowa z Podprzetwarzającym musi być zawarta w tej samej formie, co niniejsza Umowa.

3. Obowiązki Przetwarzającego

Przetwarzający ma następujące obowiązki:

- 3.1. **Udokumentowane polecenia [art. 28 ust. 3 lit. a RODO]** Przetwarzający przetwarza Dane wyłącznie zgodnie z niniejszą Umową i udokumentowanymi poleceniami lub instrukcjami Administratora.
- 3.2. **Nieprzetwarzanie poza EOG [art. 28 ust. 3 lit. a RODO]** Przetwarzający oświadcza, że nie przekazuje Danych do państwa trzeciego lub organizacji międzynarodowej (czyli poza Europejski Obszar Gospodarczy („EOG”). Przetwarzający oświadcza również, że nie korzysta z podwykonawców, którzy przekazują Dane poza EOG.
- 3.3. **Poinformowanie o zamiarze przetwarzania poza EOG. [art. 28 ust. 3 lit. a RODO]** Jeżeli Przetwarzający ma zamiar lub obowiązek przekazywać Dane poza EOG, informuje o tym Administratora, w celu umożliwienia Administratorowi podjęcia decyzji i działań niezbędnych do zapewnienia zgodności przetwarzania z prawem lub zakończenia powierzenia przetwarzania.
- 3.4. **Tajemnica [art. 28 ust. 3 lit. b RODO]** Przetwarzający uzyskuje od osób, które zostały upoważnione do przetwarzania Danych w wykonaniu Umowy, udokumentowane zobowiązania do zachowania tajemnicy, ewentualnie upewnia się, że te osoby podlegają ustawowemu obowiązkowi zachowania tajemnicy.
- 3.5. **Bezpieczeństwo [art. 28 ust. 3 lit. c RODO]** Przetwarzający zapewnia ochronę Danych i podejmuje środki ochrony danych, o których mowa w art. 32 RODO, zgodnie z dalszymi postanowieniami Umowy.
- 3.6. **Współpraca przy realizacji praw jednostki [art. 28 ust. 3 lit. e RODO]** Przetwarzający zobowiązuje się do realizacji obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO. W szczególności Przetwarzający

zobowiązuje się, na żądanie Administratora, do przygotowania i przekazania Administratorowi informacji potrzebnych do spełnienia żądania osoby, której dane dotyczą, w ciągu 3 dni od dnia otrzymania żądania Administratora.

- 3.7. **Wsparcie przy obowiązkach bezpieczeństwa [art. 28 ust. 3 lit. f RODO]** Przetwarzający współpracuje z Administratorem przy wykonywaniu przez Administratora obowiązków z obszaru ochrony danych osobowych, o których mowa w art. 32–36 RODO (ochrona danych, zgłaszanie naruszeń organowi nadzorczemu, zawiadamianie osób dotkniętych naruszeniem ochrony danych, ocena skutków dla ochrony danych i uprzednie konsultacje z organem nadzorczym).
- 3.8. **Legalność poleceń [art. 28 ust. 3 ak. 2 RODO]** Jeżeli Przetwarzający poweźmie wątpliwości co do zgodności z prawem wydanych przez Administratora poleceń lub instrukcji, Przetwarzający natychmiast informuje Administratora o stwierdzonej wątpliwości (w sposób udokumentowany i z uzasadnieniem), pod rygorem utraty możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu.
- 3.9. **Projektowanie prywatności [art. 25 ust. 1 RODO]** Planując dokonanie zmian w sposobie przetwarzania Danych, Przetwarzający ma obowiązek zastosować się do wymogu projektowania prywatności, o którym mowa w art. 25 ust. 1 RODO i ma obowiązek z wyprzedzeniem informować Administratora o planowanych zmianach w taki sposób i terminach, aby zapewnić Administratorowi realną możliwość reagowania, jeżeli planowane przez Przetwarzającego zmiany w opinii Administratora grożą uzgodnionemu poziomowi bezpieczeństwa Danych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek przetwarzania Danych przez Przetwarzającego.
- 3.10. **Minimalizacja [art. 25 ust. 2 RODO]** Przetwarzający zobowiązuje się do ograniczenia dostępu do Danych Osobowych wyłącznie do osób, których dostęp do Danych jest potrzebny dla realizacji Umowy i posiadających odpowiednie upoważnienie.
- 3.11. **RCPD [art. 30 ust. 2 RODO]** Przetwarzający zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania Danych, zgodnie z RODO.
- 3.12. **Profilowanie [art. 13 i 14 RODO]** Jeżeli Przetwarzający wykorzystuje, zgodnie z Umową Podstawową, zautomatyzowane przetwarzanie, w tym profilowanie, o którym mowa w art. 22 ust. 1 i 4 RODO, Przetwarzający informuje o tym Administratora w celu i w zakresie niezbędnym do wykonania przez Administratora obowiązku informacyjnego.
- 3.13. **Kontrole.** Przetwarzający zobowiązuje się do każdorazowego informowania Administratora (na adres e-mail: iod@wsb.warszawa.pl) o przeprowadzanych w jego podmiocie kontrolach organu nadzorczego w obszarze ochrony danych osobowych.

4. Obowiązki Administratora

Administrator zobowiązany jest współdziałać z Przetwarzającym w wykonaniu Umowy, udzielać Przetwarzającemu wyjaśnień w razie wątpliwości co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków.

5. Bezpieczeństwo danych

- 5.1. **Bezpieczeństwo danych osobowych [art. 32 RODO]** Przetwarzający przeprowadził analizę ryzyka przetwarzania powierzonych Danych i stosuje się do jej wyników co do organizacyjnych i technicznych środków ochrony danych oraz udostępni ją Administratorowi na jego wniosek.
- 5.2. **Gwarancje bezpieczeństwa.** Przetwarzający:
 - (1) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania zgodności działania Administratora z przepisami RODO,

- (2) umożliwia Administratorowi lub upoważnionemu przez niego audytorowi przeprowadzanie audytów lub inspekcji. Przetwarzający współpracuje w zakresie realizacji audytów lub inspekcji.

6. Powiadomienie o Naruszeniach Danych Osobowych

- 6.1. **Powiadomienie o naruszeniu.** Przetwarzający powiadamia Administratora danych o każdym podejrzeniu naruszenia ochrony Danych osobowych nie później niż w 24 godziny od pierwszego zgłoszenia, umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających i informuje Administratora o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu naruszenia.
- 6.2. **Rozwinięcie.** Powiadomienie o stwierdzeniu naruszenia, powinno być przesłane wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organ nadzoru. Na żądanie Administratora Przetwarzający zobowiązany jest do przesłania uzupełniającej dokumentacji dotyczącej naruszenia.
- 6.3. Przetwarzający zobowiązuje się do przeprowadzenia wstępnej analizy ryzyka naruszenia praw i wolności osób, których dane dotyczą, i przekazania wyników tej analizy do Administratora w ciągu 36 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony danych osobowych.
- 6.4. Powiadomienia o Naruszeniach Danych Osobowych wysyłane są na następujący adres mailowy: iod@wsb.warszawa.pl

7. Nadzór

- 7.1. **Sprawowanie kontroli [art. 28 ust. 3 lit. h RODO]** Administrator kontroluje sposób przetwarzania powierzonych Danych Osobowych po uprzednim poinformowaniu Przetwarzającego o planowanej kontroli. Administrator lub wyznaczone przez niego osoby są uprawnione do (i) wstępu do pomieszczeń, w których przetwarzane są Dane Osobowe oraz (ii) wglądu do dokumentacji związanej z przetwarzaniem Danych Osobowych. Administrator uprawniony jest do żądania od Przetwarzającego udzielania informacji dotyczących przebiegu przetwarzania Danych Osobowych, oraz udostępnienia rejestrów przetwarzania.
- 7.2. **Współpraca przy kontroli. [art. 28 ust. 3 lit. h RODO]** Przetwarzający współpracuje z urzędem nadzoru w obszarze ochrony danych osobowych w zakresie wykonywanych przez niego zadań.

8. Oświadczenia Stron

- 8.1. **Oświadczenie Administratora.** Administrator oświadcza, że jest Administratorem Danych oraz, że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.
- 8.2. **Oświadczenie Przetwarzającego [art. 28 ust. 1 RODO].** Przetwarzający oświadcza, że posiada w zakresie przetwarzania danych osobowych niezbędną wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego wykonania niniejszej Umowy.
- 8.3. **Gwarancje [art. 28 ust. 1 RODO].** Na żądanie Administratora Przetwarzający okaże Administratorowi, iż zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

9. Odpowiedzialność

- 9.1. **Odpowiedzialność Przetwarzającego [art. 82 ust. 3 RODO]** Przetwarzający odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Przetwarzającego lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom. Przetwarzający odpowiada za szkody spowodowane zastosowaniem lub nie zastosowaniem właściwych środków bezpieczeństwa.

- 9.2. **Odpowiedzialność za Podprzetwarzających [art. 28 ust. 4 RODO]** Jeżeli Podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków przez Podprzetwarzającego spoczywa na Przetwarzającym.
- 9.3. **Odpowiedzialność Przetwarzającego** W przypadku naruszenie przepisów RODO lub Umowy z przyczyn leżących po stronie Przetwarzającego, w następstwie czego Administrator zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą administracyjną, przewidzianą w RODO, Przetwarzający zobowiązuje się pokryć Administratorowi poniesione z tego tytułu wszelkie straty i koszty, w tym koszty postępowań.

10. Okres Obowiązkiwania Umowy Powierzenia [art. 28 ust. 3 RODO]

Umowa została zawarta na czas obowiązywania Umowy Podstawowej, przy czym zapisy Umowy pozostają w mocy do czasu spełnienia wszystkich obowiązków wynikających z RODO przez Przetwarzającego.

11. Usunięcie Danych

- 11.1. **Usunięcie Danych [art. 28 ust. 3 lit g RODO]** Z chwilą rozwiązania Umowy, Przetwarzający nie ma prawa do dalszego przetwarzania powierzonych Danych i jest zobowiązany do usunięcia Danych i usunięcia wszelkich ich istniejących kopii lub zwrotu Danych, w zależności od żądania Administratora.
- 11.2. **Oświadczenie.** Po wykonaniu zobowiązania, o którym mowa w pkt 11.1., Przetwarzający złoży Administratorowi pisemne oświadczenie potwierdzające wykonanie tego obowiązku.

12. Postanowienia Końcowe

- 12.1. Niniejsza Umowa zastępuje wszelkie dotychczasowe postanowienia dotyczące ochrony danych osobowych zawarte w Umowie Podstawowej.
- 12.2. **Egzemplarze.** Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
- 12.3. **Forma.** Wszelkie zmiany niniejszej Umowy Powierzenia wymagają dla swojej ważności formy pisemnej.
- 12.4. **Właściwość prawa.** Umowa podlega prawu polskiemu oraz RODO.

.....
podpis Administratora

.....
podpis Przetwarzającego

Załącznik:

- Ankieta dla podmiotu przetwarzającego



Ankieta dla Podmiotu Przetwarzającego

Zgodnie z art. 28 ust. 1 RODO, Wyższa Szkoła Bankowa jako Administrator Danych Osobowych, jest odpowiedzialna za korzystanie z usług wyłącznie takich podmiotów przetwarzających, które gwarantują wdrożenie odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi ogólnego rozporządzenia o ochronie danych i chroniło prawa osób, których dane dotyczą.

Poniższa ankieta jest narzędziem pozwalającym przeanalizować możliwość powierzenia Państwu danych osobowych w zakresie i w związku z wykonywaniem umowy podstawowej. Dostęp do uzupełnionej ankiety posiadają jedynie osoby odpowiedzialne za procesy związane z ochroną danych osobowych w podmiocie. Pragniemy również zapewnić, że uzupełnione przez Państwa informacje traktujemy, jako dane poufne i nie będą one przekazywane innym osobom.

Pytania z ankiety

1. Nazwa Podmiotu Przetwarzającego
2. Osoba odpowiedzialna za umowę ze strony Wyższej Szkoły Bankowej
3. Czy osoby wykonujące operacje na danych osobowych otrzymały od podmiotu przetwarzającego upoważnienia do przetwarzania danych, w których został określony w szczególności zakres przetwarzanych przez te osoby danych.
4. Czy podmiot powołał Inspektora Ochrony Danych?
5. Kontakt do Inspektora Ochrony Danych
6. Czy podmiot przetwarzający prowadzi rejestr czynności oraz kategorii czynności przetwarzania?
7. Czy podmiot prowadzi ocenę skutków dla ochrony danych?
8. Czy podmiot okresowo dokonuje przeglądu ryzyk związanych z przetwarzaniem danych osobowych?
9. Czy w przypadku zmiany poziomu ryzyka podmiot dobiera nowe/odpowiednie środki techniczne i organizacyjne zabezpieczające dane, stosownie do wyników analizy?
10. Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych?
11. Czy podmiot wdrożył inne zasady, standardy, regulaminy, procedury, polityki, biblioteki lub zbiory najlepszych praktyk mające znaczenie dla ochrony informacji/danych osobowych?
12. Czy podmiot dba o bieżące doskonalenie wiedzy swoich pracowników poprzez cykliczne szkolenia oraz inne działania mające na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych?
13. Czy pracownicy podmiotu, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy?
14. Czy podmiot korzysta z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych?
15. Czy podmiot zapewnił fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez organizację od tych, które należą do innych organizacji?
16. Czy dane osobowe gromadzone w formie papierowej, po godzinach pracy organizacji, przechowywane są w bezpieczny sposób bez możliwości dostępu do nich osób nieupoważnionych?
17. Czy podmiot zapewnił aktualne oprogramowanie antywirusowe na wszystkich stacjach?
18. Czy podmiot stosuje szyfrowanie dysków komputerów przenośnych?



19. Czy podmiot stosuje rozwiązania chmurowe?
20. Czy dostawca został zweryfikowany pod kątem RODO?
21. Czy dane są przekazywane w chmurze poza obszar EOD?
22. Czy podmiot posiada procedury odtwarzania systemu po awarii oraz ich testowania?
23. Jaki przyjęto zakres oraz częstotliwość tworzenia kopii zapasowych?
24. Czy podmiot wdraża nowe rozwiązania zgodnie z zasadą "privacy by design"?
25. Czy podmiot działa zgodnie z zasadą "privacy by default"?
26. Czy podmiot przetwarzający prowadzi regularnie audyty dotyczące zasad bezpieczeństwa informacji?
27. Czy wnioski z audytów zostały udokumentowane, np. w raporcie audytowym?
28. Czy podmiot jest przygotowany do poddania się audytowi przeprowadzonemu przez administratora danych lub audytora upoważnionego przez administratora danych?
29. Czy podmiot gwarantuje realizację praw osób, których dane dotyczą tj. m.in. prawo do przenoszenia danych, prawo do ograniczania przetwarzania, prawo do bycia zapomnianym?
30. Czy podmiot wdrożył procedurę/instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych?
31. Czy podmiot jest w stanie wykazać rozliczalność podjętych działań na danych osobowych powierzonych przez Administratora?
32. Czy były przeprowadzane kontrole przez UODO (kompleksowe, sektorowe, ze skargi lub w wyniku zaistnienia naruszenia)?
33. Czy podmiot prowadzi rejestr naruszeń i incydentów?
34. Czy podmiot wdrożył mechanizmy usuwania danych po zakończeniu celu przetwarzania?
35. Czy podmiot przekazuje dane osobowe do państwa trzeciego?