

Załącznik nr 1 do UPPDO

Arkusz weryfikacji przeznaczony dla podmiotu przetwarzającego

Nazwa Działu merytorycznie odpowiedzialnego za umowę główną i podpisanie do niej umowy powierzenia przetwarzania danych osobowych	Dział Osobą wyznaczoną do kontaktu ze strony Administratora w związku z realizacją Umowy PPDO oraz wykonywaniem wskazanych w niej uprawnień i obowiązków jest: imię i nazwisko (stanowisko): adres e-mail: tel.: adres do korespondencji:
Dane (potencjalnego) podmiotu przetwarzającego (Nazwa, forma prawna, siedziba, adres do doręczeń, NIP, REGON, KRS, adres email.)	Osobą wyznaczoną do kontaktu ze strony podmiotu przetwarzającego w związku z realizacją Umowy PPDO oraz wykonywaniem wskazanych w niej uprawnień i obowiązków jest: imię i nazwisko (stanowisko): adres e-mail: tel.: adres do korespondencji:
Przedmiot umowy, zakres współpracy	



Fundusze Europejskie
dla Nowoczesnej Gospodarki



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Ministerstwo Nauki
i Szkolnictwa Wyższego

Wykaz środków organizacyjnych i technicznych stosowanych przez (potencjalny) Podmiot przetwarzający

Lp.	Pytanie	Odpowiedź – wyłącznie w formie opisowej	Ocena zgodności z wymogami ochrony danych osobowych wynikającymi z RODO (wypełnia Administrator z podaniem daty)	Uwagi (wypełnia Administrator)
1	Czy przetwarzający zapewnia, że nowo zatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych jest szkoleny w tym zakresie i zapoznany z obowiązującymi przepisami prawa?		Zgodność/niezgodność	
2	Czy przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników dzięki cyklicznym szkoleniom oraz innym działaniom mającym na celu uświadamianie swoich pracowników w zakresie zagadnień dotyczących ochrony danych osobowych? Proszę o wskazanie daty ostatniego szkolenia.		Zgodność/niezgodność	
3	Czy przetwarzający zapewnia, że wszyscy jego pracownicy zaangażowani w operacje przetwarzania danych osobowych posiadają pisemne upoważnienia do przetwarzania danych osobowych?		Zgodność/niezgodność	
4	Czy przetwarzający zapewnia, że wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych zostały przez niego zobowiązane do zachowania w tajemnicy danych osobowych oraz sposobu ich zabezpieczenia, zarówno w trakcie zatrudnienia jak i po jego ustaniu?		Zgodność/niezgodność	



Fundusze Europejskie
dla Nowoczesnej Gospodarki



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Ministerstwo Nauki
i Szkolnictwa Wyższego

5	Czy przetwarzający posiada obowiązek powołania inspektora ochrony danych osobowych? Jeśli tak, czy przetwarzający powołał inspektora ochrony danych osobowych? (Proszę o wskazanie imienia i nazwiska Inspektora ochrony danych, adres mailowy i nr telefonu, a także link do strony gdzie zostały opublikowane dane inspektora zgodnie z art. 11 ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.) Jeśli przetwarzający nie posiada obowiązku powołania inspektora ochrony danych, czy powołał co najmniej jedną osobę odpowiedzialną za ochronę danych osobowych, z którą administrator może kontaktować się w związku z realizacją umowy powierzenia przetwarzania danych osobowych? (Proszę o wskazanie imienia i nazwiska tej osoby, adres mailowy i nr telefonu).		Zgodność/niezgodność	
6	Czy przetwarzający opracował i wdrożył politykę/procedurę ochrony danych osobowych, w tym procedurę dotyczącą sposobu działania w przypadku wystąpienia incydentu naruszenia danych osobowych oraz umożliwiającą realizację praw osób, których dane osobowe dotyczą? Jeśli zostały stworzone, należy je wskazać z krótkim opisem ich zastosowania.		Zgodność/niezgodność	
7	Czy w ciągu ostatnich dwóch lat podmiot przetwarzający poddawał zewnętrżnej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych?		Zgodność/niezgodność	
8	Czy u przetwarzającego przeprowadzono kontrolę z Urzędu Ochrony Danych Osobowych? Jeśli tak, należy wskazać, jaki był wynik kontroli.		Zgodność/niezgodność	
9	Czy przetwarzający w sposób bieżący prowadzi rejestr czynności przetwarzania danych osobowych i rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora?		Zgodność/niezgodność	



Fundusze Europejskie
dla Nowoczesnej Gospodarki



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Ministerstwo Nauki
i Szkolnictwa Wyższego

10	Czy przetwarzający opracował i wdrożył procedurę dotyczącą sposobu działania w przypadku wystąpienia incydentu naruszenia danych osobowych? Proszę o wskazanie nazwy ww. dokumentu wraz z datą zatwierdzenia oraz nadanym numerem wewnętrznym.		Zgodność/niezgodność	
11	Czy u przetwarzającego miało miejsce naruszenie ochrony danych osobowych? Jeżeli tak, proszę opisać, czego dotyczyło ostanie naruszenie i jakie skutki miało oraz jakie zostały podjęte działania zaradcze.		Zgodność/niezgodność	
12	Czy podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? Jeśli tak, to w jaki sposób są oni weryfikowani? Czy przetwarzający zawarł z nimi umowy powierzenia przetwarzania danych osobowych?		Zgodność/niezgodność	
13	Czy przetwarzający w ramach swojej działalności przekazuje dane osobowe poza Unię Europejską/Europejski Obszar Gospodarczy (w tym, czy Przetwarzający przechowuje dane osobowe na serwerach zlokalizowanych poza Unią Europejską/Europejskim Obszarem Gospodarczym)? Jeśli tak, należy wskazać kraj, do którego dane są przekazywane i środki służące zabezpieczeniu ich przetwarzania.		Zgodność/niezgodność	
14	Czy podmiot przetwarzający wdrożył regulacje w zakresie ruchu osobowo-materiałowego?		Zgodność/niezgodność	
15	Czy dane osobowe powierzone przez NCBR będą logicznie lub fizycznie oddzielone od innych danych przetwarzanych przez podmiot przetwarzający?		Zgodność/niezgodność	
16	Czy podmiot przetwarzający stosuje fizyczne zabezpieczenia pomieszczeń/obszarów przetwarzania danych osobowych przed dostępem osób nieuprawnionych? Jeśli tak, proszę opisać jakie.		Zgodność/niezgodność	



Fundusze Europejskie
dla Nowoczesnej Gospodarki



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Ministerstwo Nauki
i Szkolnictwa Wyższego

17	Czy podmiot przetwarzający prowadzi ewidencję gości wchodzących na teren podmiotu?		Zgodność/niezgodność	
18	Czy goście mogą przebywać na terenie podmiotu przetwarzającego tylko w obecności upoważnionych pracowników?		Zgodność/niezgodność	
19	Czy przetwarzający opracował i wdrożył formalne zasady przetwarzania danych osobowych w systemach informatycznych? Proszę o wskazanie nazwy ww. dokumentu wraz z datą zatwierdzenia oraz nadanym numerem wewnętrznym.		Zgodność/niezgodność	
20	Czy podmiot przetwarzający wdrożył formalne zasady zarządzania uprawnieniami w systemach IT? Proszę o wskazanie nazwy ww. dokumentu wraz z datą zatwierdzenia oraz nadanym numerem wewnętrznym.		Zgodność/niezgodność	
21	Czy każdy pracownik/współpracownik podmiotu przetwarzającego otrzymuje imienny identyfikator do systemów informatycznych?		Zgodność/niezgodność	
22	Czy wprowadzono zasady bezpiecznego korzystania z haseł przez użytkowników?		Zgodność/niezgodność	
23	Czy systemy informatyczne wykorzystywane przez podmiot przetwarzający zapewniają wymuszanie na użytkownikach okresowej zmiany haseł oraz zmian w razie zaistniałej potrzeby?		Zgodność/niezgodność	
24	Czy pracownicy/współpracownicy podmiotu przetwarzającego zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów, poprzez blokadę ekranu lub w inny równoważny sposób?		Zgodność/niezgodność	
25	Czy pracownicy podmiotu przetwarzającego mogą mieć zdalny dostęp do danych osobowych powierzonych przez NCBR?		Zgodność/niezgodność	



Fundusze Europejskie
dla Nowoczesnej Gospodarki



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Ministerstwo Nauki
i Szkolnictwa Wyższego

26	Czy podmiot przetwarzający wprowadził zasady dotyczące bezpiecznej pracy zdalnej? Proszę o wskazanie nazwy ww. dokumentu wraz z datą zatwierdzenia oraz nadanym numerem wewnętrznym.		Zgodność/niezgodność	
27	Czy przy dostępie zdalnym wymagana jest autoryzacja wieloskładnikowa (MFA)?		Zgodność/niezgodność	
28	Czy podmiot przetwarzający zapewnia rozliczalność działań podejmowanych przez użytkowników systemów informatycznych, np. czy istnieje możliwość stwierdzenia, kto i kiedy modyfikował dane konkretnej osoby lub miał do nich wgląd?		Zgodność/niezgodność	
29	Czy podmiot przetwarzający wdrożył formalne zasady monitorowania systemów informatycznych? Proszę o wskazanie nazwy ww. dokumentu wraz z datą zatwierdzenia oraz nadanym numerem wewnętrznym.		Zgodność/niezgodność	
30	Czy podmiot przetwarzający wdrożył zapory sieciowe kontrolujące wymianę danych z Internetem i innymi zewnętrznymi sieciami, z uwzględnieniem filtracji ruchu wchodzącego i wychodzącego?		Zgodność/niezgodność	
31	Czy podmiot przetwarzający wdrożył bezpieczne mechanizmy szyfrowania przesyłanych danych, zgodne z zaleceniami NIST SP800-131A?		Zgodność/niezgodność	
32	Czy podmiot przetwarzający wprowadził bezpieczne (zgodne z NIST SP800-131A) mechanizmy szyfrowania danych, przechowywanych na przenośnych urządzeniach końcowych, tym laptopach?		Zgodność/niezgodność	
33	Czy powierzone przez NCBR dane będą przechowywane przez podmiot przetwarzający na nośnikach przenośnych?		Zgodność/niezgodność	
34	Czy podmiot przetwarzający zapewnia, że nośniki przenośne zawierające dane osobowe podlegają szyfrowaniu z wykorzystaniem mechanizmów zgodnych z NIST SP800-131A?		Zgodność/niezgodność	
35	Czy zastosowano oprogramowanie antywirusowe na wszystkich stacjach wykorzystywanych przez pracowników/współpracowników podmiotu przetwarzającego?		Zgodność/niezgodność	



Fundusze Europejskie
dla Nowoczesnej Gospodarki



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



36	Czy zastosowano oprogramowanie antywirusowe na wszystkich serwerach podmiotu przetwarzającego, na których będą przetwarzane dane osobowe powierzone przez NCBR?		Zgodność/niezgodność	
37	Czy zastosowano inne środki techniczne zapewniające ochronę przez złośliwym oprogramowaniem? Jeśli tak, to jakie?		Zgodność/niezgodność	
38	Czy pracownicy podmiotu przetwarzającego podlegają szkoleniom z zakresu unikania ryzyka związanego z występowaniem i działaniem złośliwego oprogramowania?		Zgodność/niezgodność	
39	Czy podmiot przetwarzający wykorzystuje oprogramowanie wyłącznie zgodnie z postanowieniami warunków licencyjnych?		Zgodność/niezgodność	
40	Czy podmiot przetwarzający wdrożył zasady utwardzania konfiguracji oprogramowania systemowego i aplikacyjnego?		Zgodność/niezgodność	
41	Czy podmiot przetwarzający wdrożył zasady identyfikowania i zarządzania podatnościami w oprogramowaniu?		Zgodność/niezgodność	
42	Czy podmiot przetwarzający wdrożył sformalizowany proces instalacji poprawek bezpieczeństwa dla eksploatowanego oprogramowania?		Zgodność/niezgodność	
43	Czy podmiot przetwarzający wdrożył sformalizowane zasady zarządzania zmianą w systemach informatycznych, uwzględniające zapewnienie należytej ochrony danych?		Zgodność/niezgodność	
44	Czy podmiot przetwarzający zapewnia nadzór nad serwisantami IT będącymi pracownikami firm zewnętrznych?		Zgodność/niezgodność	
45	Czy podmiot przetwarzający zapewnił pozostawianie uszkodzonych nośników danych (zamiast oddawania ich firmie serwisowej w celu wymiany na sprawny nośnik)?		Zgodność/niezgodność	



Fundusze Europejskie
dla Nowoczesnej Gospodarki



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Ministerstwo Nauki
i Szkolnictwa Wyższego

46	Czy podmiot przetwarzający wdrożył metody bezpiecznego usuwania danych z nośników wycofanych z eksploatacji? Jeśli tak, to jakie?		Zgodność/niezgodność	
47	Jaki zakres oraz częstotliwość tworzenia kopii zapasowych danych przyjął podmiot przetwarzający?		Zgodność/niezgodność	
48	Czy kopie zapasowe przechowywane są w sposób umożliwiający zapewnienie ciągłości działania?		Zgodność/niezgodność	
49	Czy podmiot przetwarzający posiada zasady odtwarzania systemu po awarii?		Zgodność/niezgodność	
50	Czy podmiot przetwarzający przeprowadza okresowe testy odtworzeniowe systemów informatycznych, w których będą przetwarzane dane osobowe? Jaka jest częstotliwość powyższych testów?		Zgodność/niezgodność	
51	Czy podmiot przetwarzający wdrożył plany ciągłości działania obejmujące procesy związane z przetwarzaniem informacji powierzonych przez NCBR?		Zgodność/niezgodność	
52	Czy podmiot przetwarzający przeprowadza regularnie, nie rzadziej niż raz na 12 miesięcy, testy i przeglądy planów ciągłości działania?		Zgodność/niezgodność	
53	Czy podmiot przetwarzający wdraża nowe rozwiązania zgodnie z zasadą "ochrony danych w fazie projektowania" (privacy by design)? W jaki sposób realizowana jest ww. zasada przez podmiot przetwarzający?		Zgodność/niezgodność	
54	Czy podmiot przetwarzający działa zgodnie z zasadą domyślnej ochrony danych (privacy by default)? W jaki sposób realizowana jest ww. zasada przez podmiot przetwarzający?		Zgodność/niezgodność	
55	Czy podmiot przeprowadza okresowo analizę ryzyka przetwarzania danych osobowych? Jeśli tak, to jak często?		Zgodność/niezgodność	



Fundusze Europejskie
dla Nowoczesnej Gospodarki



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Ministerstwo Nauki
i Szkolnictwa Wyższego

56	Czy podmiot przetwarzający prowadzi ocenę skutków dla ochrony danych?		Zgodność/niezgodność	
57	Czy dane osobowe powierzone przez NCBR będą przetwarzane przez podmiot przetwarzający z wykorzystaniem chmury obliczeniowej, innej niż chmura prywatna?		Zgodność/niezgodność	
58	Czy dane osobowe powierzone przez NCBR będą przetwarzane przez podmiot przetwarzający w celu przeprowadzania testów?		Zgodność/niezgodność	
59	Czy przetwarzający opracował i wdrożył procedurę umożliwiającą realizację praw osób, których dane osobowe dotyczą? Proszę o wskazanie nazwy ww. dokumentu wraz z datą zatwierdzenia oraz nadanym numerem wewnętrznym.		Zgodność/niezgodność	
60	Czy systemy informatyczne wykorzystywane przez podmiot przetwarzający do przetwarzania danych osobowych powierzonych przez NCBR zapewniają, że dla każdej osoby, której dane są przetwarzane, możliwe jest trwałe usunięcia tych danych?		Zgodność/niezgodność	



Fundusze Europejskie
dla Nowoczesnej Gospodarki



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Ministerstwo Nauki
i Szkolnictwa Wyższego

Wykaz podwykonawców potencjalnego Podmiotu przetwarzającego (podprocesorów)

Czy Podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego (podprocesorów)?		
☐ TAK		☐ NIE
Jeśli zaznaczono TAK , proszę o wypełnienie poniższych wierszy		
PODPROCESOR		
Nazwa i dane kontaktowe innego (dalszego) podmiotu przetwarzającego (Podprocesora) (adres siedziby, adres e.mail, strona www, nr telefonu itp.)	• Cel dalszego powierzenia przetwarzania danych osobowych • Czynności przetwarzania, które są realizowane przez dalszy podmiot przetwarzający • Kategorie i zakres danych, które podlegają podpowierzeniu	Dane Inspektora Ochrony Danych lub osoby wyznaczonej do kontaktu w zakresie ochrony danych osobowych (imię, nazwisko, nr telefonu, adres email, link do strony gdzie zostały opublikowane dane inspektora zgodnie z art. 11 Ustawy o ochronie danych osobowych)



Fundusze Europejskie
dla Nowoczesnej Gospodarki



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Ministerstwo Nauki
i Szkolnictwa Wyższego

.....
Data i podpis osoby reprezentującej (potencjalny) podmiot przetwarzający