ANKIETA – WYMAGANIA DLA PODMIOTU ZEWNĘTRZNEGO

w zakresie możliwości powierzenia przetwarzania danych osobowych

Poniższa ankieta ma na celu ustalenie czy podmiot zewnętrzny, któremu ARiMR zamierza powierzyć przetwarzanie danych osobowych, zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odbywało się zgodnie z RODO i chroniło prawa osób, których dane dotyczą. W tym celu należy odpowiedzieć na poniższe pytania.

1. SYSTEMY OCHRONY DANYCH, KODEKSY POSTĘPOWANIA, CERTYFIKACJA

1) Czy Podmiot zewnętrzny ma wdrożony system zarządzania bezpieczeństwem informacji lub znak jakości i oznaczeń w zakresie ochrony danych osobowych, o których mowa w art. 42 RODO, i które obejmują całość operacji przetwarzania danych w ramach realizacji Umowy?

   TAK/NIE

2) Czy Podmiot zewnętrzny wdrożył i stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO?

   TAK/NIE

3) Czy system ochrony danych osobowych Podmiotu zewnętrznego był poddawany w ciągu ostatnich 3 lat sprawdzeniu przez audytorów zewnętrznych i uzyskał pozytywną opinię w tym zakresie (np.: posiada certyfikat zgodności systemu zarządzania bezpieczeństwem informacji z normą ISO/IEC 27001 w pełnym zakresie)?

   TAK/NIE

1.1. Wymagania do pkt 1

a) W przypadku pozytywnej odpowiedzi na pytanie zawarte w pkt 3, Podmiot zewnętrzny zobowiązany jest do dostarczenia **kopii certyfikatu**, o którym mowa w pytaniu pkt 3.

b) W przypadku pozytywnej odpowiedzi na pytanie zawarte w pkt 1 lub 2 przy jednoczesnej negatywnej odpowiedzi na pytanie pkt 3, Podmiot zewnętrzny zobowiązany jest do dostarczenia obowiązujących w organizacji odpowiednio: **kodeksu postępowania** lub **zasad ochrony danych osobowych** (np. polityki bezpieczeństwa informacji).

W przypadku negatywnych odpowiedzi na pytania zawarte w pkt 1 – 3 należy odpowiedzieć na pytania zawarte w kolejnych punktach.

2. STRUKTURA OCHRONY DANYCH, DOŚWIADCZENIE

1) Czy Podmiot zewnętrzny posiada doświadczenie w świadczeniu usług polegających na zarządzaniu zbiorami danych osobowych w imieniu innego podmiotu (pełnił rolę podmiotu przetwarzającego)?

TAK*/NIE

* Jeśli TAK, to proszę wskazać dla ilu pomiotów była taka usługa świadczona i przez jaki okres (łącznie, np.: 5 podmiotów, 8 lat):.....

2) Czy w trakcie świadczenia usług, o których mowa w pytaniu zawartym w pkt 1 doszło do naruszenia ochrony danych osobowych w zakresie powierzonych danych z winy podmiotu przetwarzającego?

TAK/NIE/NIE DOTYCZY

3) Czy Podmiot zewnętrzny wyznaczył w strukturach wewnętrznych Inspektora Ochrony Danych lub osobę/komórkę odpowiedzialną za nadzór nad ochroną danych osobowych? (właściwe zaznaczyć)

TAK – Inspektor Ochrony Danych (IOD)	
TAK – osoba (inna niż IOD)/ komórka odpowiedzialna za ochronę danych osobowych	
NIE	

4) Czy Podmiot zewnętrzny opracował i wdrożył metodykę oraz procedury zarządzania ryzykiem związanym z bezpieczeństwem informacji w tym metodykę oraz procedury przeprowadzania oceny skutków dla ochrony danych?

TAK/NIE

5) Czy Podmiot zewnętrzny prowadzi rejestr czynności przetwarzania spełniający wymogi przepisu art. 30 ust. 1 RODO?

TAK/NIE

6) Czy Podmiot zewnętrzny prowadzi rejestr kategorii czynności przetwarzania spełniający wymogi przepisu art. 30 ust. 2 RODO?

TAK/NIE

7) Czy Podmiot zewnętrzny przeprowadza regularne (co najmniej raz w roku) testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania?

TAK/NIE

8) Czy Podmiot przetwarzający gwarantuje realizację praw osób, których dane dotyczą, określonych w art. 15 - 22 RODO?

TAK/NIE

3. ZASADY OCHRONY DANYCH

3.1. DOSTĘP DO DANYCH

1) Czy Podmiot zewnętrzny zapewnia, aby każdy nowozatrudniony pracownik przed rozpoczęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami o ochronie danych osobowych, w tym wewnętrznymi?

TAK/NIE

2) Czy podmiot przetwarzający prowadzi cykliczne szkolenia doskonalące dla swojego personelu lub podejmuje inne działania mające na celu podnoszenie świadomości pracowników i uaktualnianie wiedzy z zakresu ochrony danych osobowych?

TAK/NIE

3) Czy osoby wykonujące operacje na danych osobowych otrzymały stosowne upoważnienia do przetwarzania danych, spełniające wymogi przepisu art. 29 RODO?

TAK/NIE

4) Czy osoby upoważnione do przetwarzania danych osobowych zostały zobowiązane do zachowania ich w tajemnicy/poufności lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy? Czy zostało to udokumentowane?

TAK (bez dokumentacji)	
TAK – udokumentowane	
NIE	

5) Czy Podmiot zewnętrzny wdrożył i stosuje w swojej organizacji sformalizowane procedury nadawania uprawnień do systemów informatycznych przetwarzających dane osobowe, z zachowaniem zasad „wiedzy koniecznej"?

TAK/NIE

6) Czy Podmiot zewnętrzny prowadzi cykliczne przeglądy nadanych uprawnień?

TAK/NIE

7) Czy Podmiot zewnętrzny wdrożył i stosuje w swojej organizacji sformalizowane procedury bezzwłocznego odbierania uprawnień do systemów informatycznych

przetwarzających dane osobowe, w stosunku do osób, dla których ustała celowość dostępu?

TAK/NIE

3.2. FIZYCZNY DOSTĘP DO OBSZARÓW PRZETWARZANIA

1) Czy Podmiot zewnętrzny stosuje środki kontroli dostępu fizycznego do budynku/budynków ograniczające dostęp tylko dla autoryzowanego personelu?

TAK/NIE

2) Czy Podmiot przetwarzający posiada odpowiednio wyposażone i zabezpieczone pomieszczenia umożliwiające bezpieczne przetwarzanie danych osobowych?

TAK/NIE

3) Czy Podmiot zewnętrzny zapewnia odpowiedni nadzór nad osobami niebędącymi jego pracownikami, a przebywającymi w jego siedzibie, także mających dostęp po godzinach pracy (personel sprzątający, personel ochrony fizycznej)?

TAK/NIE

4) Czy zapewniono fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez organizację od tych, które należą do innych organizacji?

TAK/NIE

3.3. OCHRONA DOMYŚLNA (PRIVACY BY DEFAULT)

1) Czy każdy pracownik otrzymuje unikalny identyfikator do systemów informatycznych?

TAK/NIE

2) w systemach informatycznych Podmiotu zewnętrznego zapewniono wymuszanie na użytkownikach stosowania haseł o odpowiedniej sile (kombinacja liter, cyfr i znaków specjalnych, min. 8 znakowe), także ich okresowej zmiany oraz zmian w razie zaistniałej potrzeby?

TAK/NIE

3) Czy Podmiot zewnętrzny wdrożył i stosuje w organizacji zasadę „czystego ekranu" polegającą na automatycznym wygaszaniu ekranu i blokowaniu systemu, po okresie bezczynności, gdzie powrót do normalnej pracy wymaga podania hasła?

TAK/NIE

4) Czy Podmiot zewnętrzny wdrożył i stosuje w organizacji zasadę „czystego biurka" polegającą na obowiązku chowania dokumentów zawierających dane osobowe do zamykanych szaf na koniec dnia pracy?

TAK/NIE

5) Czy w systemach informatycznych Podmiotu zewnętrznego wykorzystywane jest jedynie oprogramowanie autoryzowane przez Kierownictwo Podmiotu zewnętrznego?
TAK/NIE

6) Czy w systemach informatycznych Podmiotu zewnętrznego są wdrożone zabezpieczenia wykrywające lub zapobiegające użyciu nieautoryzowanego oprogramowania?

TAK/NIE

7) Czy systemy informatyczne Podmiotu zewnętrznego są objęte rzeczywistą ochroną przed szkodliwym oprogramowaniem (zainstalowane i regularnie uaktualniane oprogramowanie antymalwerowe na wszystkich urządzeniach wykorzystywanych do przetwarzania danych, w tym telefonach komórkowych)?

TAK/NIE

8) Czy Podmiot zewnętrzny posiada wdrożony proces zarządzania podatnościami technicznymi, mający na celu redukowanie podatności, które mogą być wykorzystane przez szkodliwe oprogramowanie lub umożliwić atak hackerski?

TAK/NIE

9) Czy posiadane przez Podmiot zewnętrzny sieci komputerowe, zarówno przewodowe jak i bezprzewodowe, poprzez odpowiednią konfigurację urządzeń i systemów, umożliwiają blokowanie podejrzanej transmisji danych?

TAK/NIE

10) Czy urządzenia mobilne (laptopy, tablety, telefony komórkowe, itp.) wykorzystywane do przetwarzania danych osobowych, którymi Podmiot zewnętrzny dysponuje, są szyfrowane?

TAK/NIE

11) Czy jest stosowane szyfrowanie komunikacji pomiędzy systemami Podmiotu zewnętrznego?

TAK/NIE

12) Czy Podmiot zewnętrzny posiada wdrożone procedury bezpiecznego zbywania sprzętu, uwzględniające całkowite usuwanie danych z nośników informacji?

TAK/NIE

13) Czy Podmiot zewnętrzny posiada wdrożony i sformalizowany proces zarządzania incydentami związanymi z bezpieczeństwem informacji?

TAK/NIE

14) Czy Podmiot zewnętrzny posiada wdrożony i sformalizowany proces zarządzania ciągłością działania?

TAK/NIE

3.4. OCHRONA NA ETAPIE PROJEKTOWANIA (PRIVACY BY DESIGN)

1) Czy posiadane przez Podmiot zewnętrzny środowiska produkcyjne, testowe oraz deweloperskie są niezależne, odseparowane od siebie, przynajmniej na poziomie VLAN-ów?

TAK/NIE

2) Czy Podmiot zewnętrzny dokonuje dla każdego projektu (dotyczącego wytworzenia nowego oprogramowania, jak również zmiany istniejącego) szacowania ryzyka pod kątem bezpieczeństwa informacji?

TAK/NIE

3) Czy Podmiot zewnętrzny wdrożył i stosuje procedury odbioru systemów przed uruchomieniem na środowisku produkcyjnym, z uwzględnieniem aspektów bezpieczeństwa informacji?

TAK/NIE

3.5. Wymagania do pkt 2 i 3

Podmiot zewnętrzny zobowiązany jest do przedłożenia stosownych zasad, procedur, o których mowa w pkt 2 i 3.

4. WERYFIKACJA ZASAD OCHRONY DANYCH

1) W przypadku udzielenia odpowiedzi negatywnej na jakiekolwiek pytanie zawarte w pkt 2 oraz 3, czy Podmiot zewnętrzny wyraża gotowość do bezzwłocznego wdrożenia brakujących zasad?

TAK/NIE

2) Czy Podmiot zewnętrzny wyraża zgodę na ewentualną weryfikację w siedzibie Podmiotu zewnętrznego, opisanych powyżej zasad ochrony danych osobowych (sposób przeprowadzenia przez ARiMR audytu będzie uzgadniany indywidualnie)?

TAK/NIE

OŚWIADCZENIE

Działając w imieniu Podmiotu Przetwarzającego potwierdzam zgodność przedstawionych powyżej informacji pod rygorem odpowiedzialności prawnej, w tym odpowiedzialności wynikającej z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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 z 04.05.2016, str. 1, Dz. Urz. UE. L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35).

.....

Data i podpis osoby upoważnionej