**Załącznik nr 4 do OSR**

**OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH**

**dla czynności prowadzenia przez Prezesa Urzędu Lotnictwa Cywilnego rejestru operatorów systemów bezzałogowych statków powietrznych**

|  |  |  |
| --- | --- | --- |
|  | Rodzaj przetwarzania danych | 1) imię i nazwisko oraz data urodzenia, w przypadku osób fizycznych oraz nazwa i numer indentyfikacyjny w przypadku osób prawnych,  2) adres, w tym adres e-mail i numer telefonu,  3) numer polisy ubezpieczeniowej |
|  | System informatyczny,  w którym przetwarzane są/będą dane osobowe | System teleinformatycznych BSP zgodnie z art. 14 ust. 1, 2, 4–6 rozporządzenia nr 2019/947/UE. |
|  | Właściciel aktywów, osoba odpowiedzialna w danej komórce organizacyjnej za konkretną czynność przetwarzania danych  i mająca prawo do podejmowania w tym zakresie decyzji. | Dyrektor Departamentu Bezzałogowych Statków Powietrznych |

**1. Opis planowanych operacji przetwarzania danych:**

|  |
| --- |
| Prezes Urzędu Lotnictwa Cywilnego (ULC) przydziela operatorowi systemu bezzałogowego statku powietrznego numer rejestracyjny oraz potwierdza wpisanie operatora systemu bezzałogowego statku powietrznego do rejestru operatorów.  Prezes ULC potwierdza wpisania operatora systemu bezzałogowego statku powietrznego do rejestru operatorów oraz wpisywanie do rejestru kompetencji i uprawnień operatorów oraz wydawanie dokumentów potwierdzających uprawnienia i kompetencje. Sprawowanie przez Prezes ULC bieżącego nadzoru nad operatorami systemów bezzałogowych statków powietrznych.  Prezes ULC, na wniosek, udostępnia nieodpłatnie dane zawarte w rejestrze operatorów Policji, Straży Granicznej, Służbie Ochrony Państwa, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnemu Biuru Antykorupcyjnemu, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu Wojskowego, Służbie Celno-Skarbowej, Służbie Więziennej, Straży Marszałkowskiej, straży gminnej (miejskiej), Żandarmerii Wojskowej, Biuru Nadzoru Wewnętrznego oraz Polskiej Agencji Żeglugi Powietrznej, w celu realizacji zadań ustawowych.  Prezes ULC dokonuje adnotacji w rejestrze operatorów na profilu operatora systemu bezzałogowego statku powietrznego, w tym na profilu pilota bezzałogowego statku powietrznego – jeżeli dotyczy, w przypadku:   1. wydania, zawieszenia albo cofnięcia potwierdzenia zaliczenia szkolenia i zdania egzaminu online, o którym mowa w art. 156p ust. 1 pkt 1; 2. wydania, zawieszenia albo cofnięcia certyfikatu kompetencji pilota bezzałogowego statku powietrznego, o którym mowa w art. 156p ust. 1 pkt 2; 3. wydania, zawieszenia albo cofnięcia certyfikatu wiedzy teoretycznej, o którym mowa w art. 156p ust. 1 pkt 3, oraz jego przedłużenia albo wznowienia, po otrzymaniu informacji od wyznaczonego podmiotu, o którym mowa w art. 156n ust. 1; 4. wydania, zmiany, zawieszenia albo cofnięcia zezwolenia na operację, o którym mowa w art. 12 ust. 2 rozporządzenia nr 2019/947/UE; 5. wydania, zawieszenia albo cofnięcia potwierdzenia odbioru i kompletności oświadczenia, o którym mowa w art. 5 ust. 5 rozporządzenia nr 2019/947/UE, lub oświadczenia o wykonywaniu operacji zgodnie z krajowym scenariuszem standardowym; 6. stwierdzenia, że zostały spełnione okoliczności, o których mowa w UAS.SPEC.085 pkt 1 i 2 części B załącznika do rozporządzenia nr 2019/947/UE; 7. wydania, zmiany, zawieszenia albo cofnięcia zezwolenia na operację, o którym mowa w art. 16 ust. 1 rozporządzenia nr 2019/947/UE; 8. wydania, zmiany, zawieszenia albo cofnięcia certyfikatu LUC; 9. wydania potwierdzenia, o którym mowa w art. 13 ust. 2 rozporządzenia nr 2019/947/UE; 10. wydania albo cofnięcia poświadczenia, o którym mowa w art. 156u ust. 3; 11. zmiany danych operatora systemu bezzałogowego statku powietrznego.   Prezes ULC wykreśla operatora systemu bezzałogowego statku powietrznego z rejestru operatorów, na wniosek operatora systemu bezzałogowego statku powietrznego albo z urzędu, w przypadku gdy operator systemu bezzałogowego statku powietrznego przestał spełniać wymagania określone w art. 14 ust. 5 lit. b rozporządzenia nr 2019/947/UE oraz nie posiada ważnych dokumentów potwierdzających kwalifikacje pilota bezzałogowego statku powietrznego, uprawniających do wykonywania operacji przy użyciu systemu bezzałogowego statku powietrznego w podkategorii A2 kategorii „otwartej”, o której mowa w art. 4 rozporządzenia nr 2019/947/UE, lub w kategorii „szczególnej”, o której mowa w art. 5 rozporządzenia nr 2019/947/UE.  Prezes ULC przechowuje dane o operatorach systemów bezzałogowych statków powietrznych wpisanych do rejestru operatorów przez 5 lat od dnia wykreślenia danego operatora systemu bezzałogowego statku powietrznego z tego rejestru. |

**2. Cel przetwarzania, w tym prawnie uzasadniony interes administratora danych:**

|  |
| --- |
| Wypełnienie obowiązku utworzenia i prowadzenia rejestru operatorów systemów bezzałogowych statków powietrznych wynikających z art. 14 rozporządzenia wykonawczego Komisji (UE) nr 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych (Dz. Urz. UE L 152 z 11.06.2019, str. 45, Dz. Urz. UE L 255 z 04.10.2019, str. 11, Dz. Urz. UE L 150 z 13.05.2020, str. 1, Dz. Urz. UE L 176 z 05.06.2020, str. 13, Dz. Urz. UE L 253 z 16.07.2021, str. 49, Dz. Urz. UE L 87 z 15.03.2022, str. 20 oraz Dz. Urz. UE L 105 z 04.04.2022, str. 3).  Skuteczny nadzór nad tymi operatorami i umożliwienie ich sprawnej identyfikacji. |

**3. Ocena, czy planowane operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów:**

|  |
| --- |
| Planowane operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów. |

**4. Ocena ryzyka naruszenia praw lub wolności osób stanowi załącznik do oceny skutków dla ochrony danych osobowych.**

**5. Środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy:**

|  |
| --- |
| Wprowadzone środki techniczne w celu zapewnienia odpowiednich zabezpieczeń, które mają wpływ na proces przetwarzania danych:   1. dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła; 2. zmiana haseł nie rzadziej niż co 30 dni; 3. zastosowanie programów antywirusowych i innych regularnie aktualizowanych narzędzi ochrony; 4. system Firewall; 5. wygaszacze ekranów; 6. automatyczna blokada dostępu do systemu w przypadku dłuższej nieaktywności pracy użytkownika; 7. systematyczne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych; 8. stosowanie indywidualnych haseł logowania do poszczególnych programów; 9. zastosowanie właściwej budowy hasła.   Wprowadzone środki organizacyjne w celu stworzenia właściwych zabezpieczeń, które wpływają na procesy przetwarzania danych są następujące:   1. przetwarzanie danych osobowych może odbywać się wyłącznie w ramach wykonywania zadań służbowych; zakres uprawnień wynika z zakresu tych zadań; 2. każdy pracownik administracji posiada wyznaczone dla siebie stanowisko komputerowe, co zmniejsza ryzyko naruszenia integralności danych osobowych; 3. pracownicy pracujący na jednym stanowisku komputerowym posiadają osobne konta użytkownika do komputera; 4. oznakowanie obszaru pracy; 5. procedury i instrukcje pracy (transport wewnętrzny i zewnętrzny, postępowanie z odpadami i zużytym sprzętem, przechowywanie materiału biologicznego, pobieranie próbek); 6. stanowiskowe instrukcje pracy (obsługa sprzętu); 7. instrukcje postępowania awaryjnego uwzględniające wszystkie możliwe drogi narażenia (rozlanie, wyciek, rozprysk, skaleczenie); 8. polityka czystego biurka.   Środki ochrony w ramach narzędzi programowych i baz danych.  Środki ochrony narzędzi programowych:   1. dostęp do systemów teleinformatycznych posiadają tylko upoważnieni użytkownicy; 2. nadawanie uprawnień oraz uwierzytelnienie użytkowników jest zgodne z rozporządzeniem; 3. stosowana jest ochrona kryptograficzna danych przesyłanych drogą teleinformatyczną; 4. zastosowane są rozwiązania chroniące systemy informatyczne przed skutkami awarii zasilania elektrycznego; 5. w celu ochrony przed złośliwym oprogramowaniem stosowane są programy antywirusowe; 6. w celu ochrony przed dostępem nieupoważnionych osób do danych osobowych drogą teleinformatyczną stosowany jest system firewall; 7. wszystkie dane osobowe przetwarzane są w macierzach dyskowych RAID np. 1, 5, 10 zabezpieczających przed skutkami awarii pamięci masowej; 8. w przypadku awarii dysku zawierającego dane osobowe dane są kasowane przy pomocy programów zamazujących dane, przed jego przekazaniem do naprawy; jeżeli naprawa dysku jest niemożliwa, po logicznym usunięciu danych jest on niszczony fizycznie; w zakresie nieuregulowanym w niniejszym dokumencie zastosowanie znajdują przepisy ustawy, rozporządzenia oraz inne przepisy prawa.   Zbiory danych osobowych przetwarzane są przy użyciu komputera stacjonarnego i przenośnego. Komputer służący do przetwarzania danych osobowych jest połączony z lokalną siecią komputerową. Stosowane są urządzenia typu UPS, i wydzielona sieć elektroenergetyczna, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania. Dostęp do zbiorów danych osobowych, które są przetwarzane na wydzielonej stacji komputerowej i komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła. Dostęp do systemu operacyjnego komputera, w którym są przetwarzane dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. Środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych. Systemowe mechanizmy wymuszają okresową zmianę haseł.  Środki kryptograficznej ochrony danych dla danych osobowych przekazywane drogą teletransmisji. Dostęp do środków teletransmisji zabezpiecza się za pomocą mechanizmów uwierzytelnienia. Stosuję się środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity. Możliwie używa się system Firewall do ochrony dostępu do sieci komputerowej.  W przypadku korzystania z systemu przez operatorów BSP oraz pilotów BSP wymagane jest dwustopniowe uwierzytelnienie przez email i SMS. Logowanie wymaga silnego hasła, a każdorazowa zmiana w systemie wymaga dwustopniowego uwierzytelnienia. |

**6. Wynik konsultacji z Inspektorem ochrony danych w Urzędzie Lotnictwa Cywilnego**

|  |
| --- |
| Na obecnym etapie prac na projektem nowelizacji ustawy z dnia 3 lipca 2002 r. - Prawo lotnicze Inspektor ochrony danych w Urzędzie Lotnictwa Cywilnego nie wniósł uwag do niniejszej oceny skutków dla ochrony danych dla opisanej czynności przetwarzania. |

**Załącznik**

**OCENA RYZYKA NARUSZENIA OCHRONY DANYCH OSOBOWYCH**

|  |  |  |
| --- | --- | --- |
|  | Czynność przetwarzania danych | Prowadzenie przez Prezesa Urzędu Lotnictwa Cywilnego (ULC) rejestru operatorów systemów bezzałogowych statków powietrznych |
|  | System informatyczny,  w którym przetwarzane są dane osobowe | System teleinformatyczny BSP na zasadach określonych w art. 14 ust. 5 rozporządzenia nr 2019/947/UE |
|  | Właściciel aktywów, osoba odpowiedzialna w danej komórce organizacyjnej za konkretną czynność przetwarzania danych  i mająca prawo do podejmowania w tym zakresie decyzji. | Dyrektor Departamentu Bezzałogowych Statków Powietrznych w ULC |

**1. Cykl „życia danych” – przetwarzanie danych na poszczególnych etapach:**

|  |  |  |
| --- | --- | --- |
| **Operacja przetwarzania danych:** | **Zakres / kategorie danych**  **osobowych** | **opis czynności realizowanych w ramach operacji przetwarzania danych** |
| zbieranie danych | 1) imię i nazwisko oraz data urodzenia, w przypadku osób fizycznych oraz nazwa i numer indentyfikacyjny w przypadku osób prawnych,  2) adres, w tym adres e-mail i numer telefonu,  3) numer polisy ubezpieczeniowej  4) numer operatora zarejestrowanego w innym kraju członkowskim UE | Prezes ULC, za pośrednictwem systemu teleinformatycznego BSP, przydziela operatorowi systemu bezzałogowego statku powietrznego numer rejestracyjny. Prezes ULC, za pośrednictwem systemu teleinformatycznego BSP, przydziela numer pilota i nadaje uzyskane kompetencje. |
| używanie danych | 1) imię i nazwisko oraz data urodzenia, w przypadku osób fizycznych oraz nazwa i numer indentyfikacyjny w przypadku osób prawnych,  2) adres, w tym adres e-mail i numer telefonu,  3) numer polisy ubezpieczeniowej  4) numer operatora zarejestrowanego w innym kraju członkowskim UE | Prezes ULC potwierdza wpisania operatora systemu bezzałogowego statku powietrznego do rejestru operatorów oraz wpisywanie do rejestru kompetencji i uprawnień operatorów oraz wydawanie dokumentów potwierdzających uprawnienia i kompetencje. Sprawowanie przez Prezes ULC bieżącego nadzoru nad operatorami systemów bezzałogowych statków powietrznych oraz kompetencjami pilotów BSP. |
| przekazywanie danych | 1) imię i nazwisko oraz data urodzenia, w przypadku osób fizycznych oraz nazwa i numer indentyfikacyjny w przypadku osób prawnych,  2) adres, w tym adres e-mail i numer telefonu,  3) numer polisy ubezpieczeniowej  4) numer operatora zarejestrowanego w innym kraju członkowskim UE | Prezes ULC, na wniosek, udostępnia nieodpłatnie dane zawarte w rejestrze operatorów Policji, Straży Granicznej, Służbie Ochrony Państwa, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnemu Biuru Antykorupcyjnemu, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu Wojskowego, Służbie Celno-Skarbowej, Służbie Więziennej, Straży Marszałkowskiej, straży gminnej (miejskiej), Żandarmerii Wojskowej, Biuru Nadzoru Wewnętrznego oraz Polskiej Agencji Żeglugi Powietrznej, w celu realizacji zadań ustawowych. |
| przechowywanie danych | 1) imię i nazwisko oraz data urodzenia, w przypadku osób fizycznych oraz nazwa i numer indentyfikacyjny w przypadku osób prawnych,  2) adres, w tym adres e-mail i numer telefonu,  3) numer polisy ubezpieczeniowej  4) numer operatora zarejestrowanego w innym kraju członkowskim UE | Prezes ULC przechowuje dane o operatorach systemów bezzałogowych statków powietrznych wpisanych do rejestru operatorów przez 5 lat od dnia wykreślenia danego operatora systemu bezzałogowego statku powietrznego z tego rejestru. |
| usuwanie danych | 1) imię i nazwisko oraz data urodzenia, w przypadku osób fizycznych oraz nazwa i numer indentyfikacyjny w przypadku osób prawnych,  2) adres, w tym adres e-mail i numer telefonu,  3) numer polisy ubezpieczeniowej  4) numer operatora zarejestrowanego w innym kraju członkowskim UE | Prezes ULC wykreśla operatora systemu bezzałogowego statku powietrznego z rejestru operatorów, na wniosek operatora systemu bezzałogowego statku powietrznego albo z urzędu, w przypadku gdy operator systemu bezzałogowego statku powietrznego przestał spełniać wymagania określone w art. 14 ust. 5 lit. b rozporządzenia nr 2019/947/UE oraz nie posiada ważnych dokumentów potwierdzających kwalifikacje pilota bezzałogowego statku powietrznego, uprawniających do wykonywania operacji przy użyciu systemu bezzałogowego statku powietrznego w podkategorii A2 kategorii „otwartej”, o której mowa w art. 4 rozporządzenia nr 2019/947/UE, lub w kategorii „szczególnej”, o której mowa w art. 5 rozporządzenia nr 2019/947/UE. |

**2. Cel przetwarzania danych osobowych:**

|  |
| --- |
| Celem przetwarzania danych w rejestrze operatorów systemów bezzałogowych statków powietrznych jest prowadzenia skutecznego nadzoru nad tymi operatorami i umożliwienia ich sprawnej identyfikacji. Docelowo system rejestracji operatorów wraz z przypisanymi kompetencjami pilotów BSP ma być połączony z repozytorium UE. Możliwa więc będzie wymiana danych pomiędzy krajami członkowskimi UE w celu weryfikacji rejestracji operatorów oraz posiadania odpowiednich kompetencji przez pilotów BSP. |

**3. Kategorie osób, których dane będą przetwarzane:**

|  |
| --- |
| Osoby fizyczne, osoby prawne oraz jednostki nieposiadające osobowości prawnej, którym przepisy nadają osobowość prawną. |

**4. Charakter przetwarzania danych osobowych:**

|  |
| --- |
| Zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie. |

**5. Stosowane środki kontroli i bezpieczeństwa:**

|  |
| --- |
| Wprowadzone środki techniczne po stronie administratorów systemu w celu zapewnienia odpowiednich zabezpieczeń, które mają wpływ na proces przetwarzania danych:   1. dostęp do systemu operacyjnego komputera, w którym są przetwarzane dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła; 2. zmiana haseł nie rzadziej niż co 30 dni; 3. zastosowanie programów antywirusowych i innych regularnie aktualizowanych narzędzi ochrony; 4. system Firewall; 5. wygaszacze ekranów; 6. automatyczna blokada dostępu do systemu w przypadku dłuższej nieaktywności pracy użytkownika; 7. systematyczne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych; 8. stosowanie indywidualnych haseł logowania do poszczególnych programów; 9. zastosowanie właściwej budowy hasła   Wprowadzone środki organizacyjne w celu stworzenia właściwych zabezpieczeń, które wpływają na procesy przetwarzania danych są następujące:   1. przetwarzanie danych osobowych może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań; 2. każdy pracownik administracji posiada wyznaczone dla siebie stanowisko komputerowe, co zmniejsza ryzyko naruszenia integralności danych osobowych; 3. pracownicy pracujący na jednym stanowisku komputerowym posiadają osobne konta użytkownika do komputera; 4. oznakowanie obszaru pracy; 5. procedury i instrukcje pracy (transport wewnętrzny i zewnętrzny, postępowanie z odpadami i zużytym sprzętem, przechowywanie materiału biologicznego, pobieranie próbek); 6. stanowiskowe instrukcje pracy (obsługa sprzętu); 7. instrukcje postępowania awaryjnego uwzględniające wszystkie możliwe drogi narażenia (rozlanie, wyciek, rozprysk, skaleczenie); 8. polityka czystego biurka.   Środki ochrony w ramach narzędzi programowych i baz danych.  Środki ochrony narzędzi programowych:   1. dostęp do systemów teleinformatycznych posiadają tylko upoważnieni użytkownicy; 2. nadawanie uprawnień oraz uwierzytelnienie użytkowników jest zgodne z rozporządzeniem; 3. stosowana jest ochrona kryptograficzna danych przesyłanych drogą teleinformatyczną; 4. zastosowane są rozwiązania chroniące systemy informatyczne przed skutkami awarii zasilania elektrycznego; 5. w celu ochrony przed złośliwym oprogramowaniem stosowane są programy antywirusowe. 6. w celu ochrony przed dostępem nieupoważnionych osób do danych osobowych drogą teleinformatyczną stosowany jest system firewall; 7. wszystkie dane osobowe przetwarzane są w macierzach dyskowych RAID np. 1, 5, 10 zabezpieczających przed skutkami awarii pamięci masowej; 8. w przypadku awarii dysku zawierającego dane osobowe, dane są kasowane przy pomocy programów zamazujących dane, przed jego przekazaniem do naprawy. Jeżeli naprawa dysku jest niemożliwa, po logicznym usunięciu danych jest on niszczony fizycznie. W zakresie nieuregulowanym w niniejszym dokumencie zastosowanie znajdują przepisy Ustawy, Rozporządzenia oraz inne przepisy prawa.   Zbiory danych osobowych są przetwarzane przy użyciu komputera stacjonarnego i przenośnego. Komputer służący do przetwarzania danych osobowych jest połączony z lokalną siecią komputerową. Stosowane są urządzenia typu UPS, i wydzielona sieć elektroenergetyczna chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania. Dostęp do zbiorów danych osobowych, które są przetwarzane na wydzielonej stacji komputerowej i komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła. Dostęp do systemu operacyjnego komputera, w którym są przetwarzane dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. Środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych. Systemowe mechanizmy wymuszają okresową zmianę haseł.  Środki kryptograficznej ochrony danych dla danych osobowych przekazywane drogą teletransmisji. Dostęp do środków teletransmisji zabezpiecza się za pomocą mechanizmów uwierzytelnienia. Stosuję się środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity. Możliwie używa się system Firewall do ochrony dostępu do sieci komputerowej.  W przypadku korzystania z systemu przez operatorów BSP oraz pilotów BSP wymagane jest dwustopniowe uwierzytelnienie przez email i SMS. Logowanie wymaga silnego hasła, a każdorazowa zmiana w systemie wymaga dwustopniowego uwierzytelnienia. |

**6. Ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Zagrożenie** | **Skutek** | **Prawdopodobieństwo** | **Wartość ryzyka** | **Poziom ryzyka** | **Postępowanie  z ryzykiem w komórce organizacyjnej** |
| Brak zagrożeń |  |  |  |  | **-** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |
| --- | --- |
| **Podsumowanie** | W wyniku oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą **nie stwierdzono** wysokiego ryzyka**.**  W związku z powyższym **nie ma konieczności** dokonania dalszej oceny skutków dla ochrony danych zgodnie z art. 35 RODO. |