WZÓR - OCENA SKUTKÓW PLANOWANYCH OPERACJI PRZETWARZANIA DLA OCHRONY DANYCH OSOBOWYCH W SYSTEMIE GEOINFO

Wersja 0.01

Warszawa, lipiec 2020 r.

Metryka dokumentu

Tytuł dokumentu:	WZÓR - Ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych w systemie GEOINFO.		
Wersja dokumentu:	0.02	**Data:**	2020-08-06
Status dokumentu:	ROBOCZY		
Stron dokumentu:	21	**Liczba załączników**	0
Plik:	Wzór - Ocena skutków planowanych operacji przetwarzania danych w systemie GEOINFO dla ochrony danych osobowych 0.02.docx		

Historia dokumentu

Wersja	Data	Osoba/osoby	Działanie
0.01	30.07.2020	Zespół projektowy MF/KAS	Opracowanie szablonu dokumentu zgodnego z wymaganiami UODO policyjnego.
0.02	06.08.2020	Zespół projektowy MF/KAS	Poprawki redakcyjne. Poprawa numeracji tabel.

Ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych w systemie GEOINFO w kontekście UODO policyjnego (in. DODO)		
Sporządził: …	Data	Podpis
Zweryfikował: …	Data	Podpis
Zatwierdził: …	Data	Podpis
Inspektor Ochrony Danych Rekomenduję/ Nie rekomenduję przetwarzania:	Data	Podpis
Opinia inspektora:		
Administrator systemu GEOINFO: Zatwierdzam	Data	Podpis

Spis treści

1 Wstęp

Niniejszy dokument stanowi WZÓR do przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, o której mowa w art. 37 ust. 1 ustawy z dnia 14 grudnia 2018r. *o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości* (Dz.U. z 2019 r. poz. 125) [UODO policyjne, in. DODO] i odnosi się do procesów przetwarzania danych i informacji z użyciem systemu GEOINFO.

2 Opis przetwarzania

Tabela 1: Opis przetwarzania danych

Lp.	Rodzaje danych	Opis
1.	Opis czynności przetwarzania	
2.	Cel przetwarzania, podstawa prawna	1)
3.	Podmioty biorące udział w przetwarzaniu (Interesariusze przetwarzania)	1)
4.	Administrator danych	
5.	Podmioty przetwarzające	1)
6.	Systemy wspierające przetwarzanie	1)
7.	Umowy powierzenia przetwarzania danych osobowych (nr umowy, z dnia, pomiędzy, na okres, w zakresie).	1)

Tabela 2: Standardy dotyczące przetwarzania danych osobowych

Standardy dotyczące przetwarzania danych (w tym normy, kodeksy postępowania, regulacje prawne)	Opis

Tabela 3 - Przesłanki wysokiego ryzyka dla praw i wolności osób

Lp.	Przesłanki wysokiego ryzyka dla praw i wolności osób	Uzasadnienie	Opis
1.	Ewaluacja lub ocena, w tym profilowanie i przewidywanie (analiza behawioralna) w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych		
2.	Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne, finansowe lub podobne istotne skutki		
3.	Systematyczne monitorowanie na dużą skale miejsc dostępnych publicznie wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdą się w monitorowanej przestrzeni.		
4.	Przetwarzanie szczególnych kategorii danych osobowych i dotyczących wyroków skazujących i czynów zabronionych (danych wrażliwych - art. 14 ust. 1 UODO policyjne)		
5.	Dane przetwarzane na dużą skalę, gdzie pojęcie dużej skali dotyczy: • liczby osób, których dane są przetwarzane, • zakresu przetwarzania, • okresu przechowywania danych oraz • geograficznego zakresu przetwarzania		
6.	Przeprowadzanie porównań, ocena lub wnioskowanie na podstawie analizy danych pozyskanych z różnych źródeł		
7.	Przetwarzanie danych dotyczących osób, których ocena i świadczone im usługi są uzależnione od podmiotów lub osób, które dysponują uprawnieniami władczymi i/lub oceniającymi		
8.	Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych		
9.	Gdy przetwarzanie samo w sobie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy		

3 Aktywa

3.1 Aktywa podstawowe

Tabela 4: Procesy przetwarzania ze wskazaniem rodzaju danych (w związku z art. 37 ust. 2 pkt 1 UODO policyjnego)

Nazwa procesu	Rodzaje danych	Odbiorcy danych	Okres retencji danych

3.2 Aktywa wspierające

Tabela 5: Identyfikacja aktywów wspierających

Przetwarzanie danych	Szczegółowy opis przetwarzania	Aktywa wspierające przetwarzanie
Gromadzenie		

Użycie		
Transfer		
Retencja		
Niszczenie		

4 Ogólna ocena ryzyka dla bezpieczeństwa informacji

…

5 Studium zasad przetwarzania danych osobowych

5.1 Środki zapewniające proporcjonalność i niezbędność przetwarzania

Tabela 6: Wyjaśnienie i uzasadnienie celów przetwarzania

Lp.	Cele przetwarzania	Uzasadnienie
1.		

5.1.1 Legalność danych

Tabela 7: Wyjaśnienie i uzasadnienie podstawy prawnej

Podstawa prawna przetwarzania	Dotyczy (TAK / NIE)	Uzasadnienie

właściwe organy przetwarzają dane osobowe wyłącznie w zakresie niezbędnym dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (art. 13 ust. 1)		
przetwarzanie danych osobowych (zebranych pierwotnie w jednym z celów) w innym nowym celu na mocy odrębnych przepisów (art. 13 ust. 2)		
przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy		
przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze		
przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej		
przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi		
przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem		

5.1.2 Minimalizacja danych

Tabela 8: Wyjaśnienie i uzasadnienie minimalizacji danych

Szczegóły dotyczące przetwarzanych danych	Kategoria danych (dane zwykłe / wrażliwe)	Uzasadnienie konieczności przetwarzania danych	Środki zapewniające minimalizację danych

5.1.3 Jakość danych

Tabela 9: Środki zapewnienia jakości danych

Środki zapewniające jakość danych	Uzasadnienie

5.1.4 Okres przechowywania

Tabela 10: Wyjaśnienie i uzasadnienie okresów przechowywania

Rodzaje danych	Okres przechowywania (retencji)	Uzasadnienie okresu przechowywania danych	Mechanizmy usuwania danych na zakończenie cyklu ich życia
Dane użytkowe			
Dane archiwalne			
Dane z dzienników systemowych			

5.2 Ocena środków w zakresie proporcjonalności i niezbędności

…

Tabela 11: Ocena środków ochrony

Środki zapewnienia zgodności z zasadami przetwarzania	Sposób realizacji	Propozycje korekty/ usprawnień
IOD: powołano i określono zadania IOD (art. 46 ust. 1 i art. 38 ust. 6 UODO policyjne)		
legalność: realizacja uprawnienia lub spełnienie obowiązku wynikającego z przepisu prawa (art. 13 UODO policyjne)		
cel lub cele: - konkretne, wyraźne i prawnie uzasadnione (art. 31 ust. 1 pkt 1 i 2 UODO policyjne)		
minimalizacja danych: adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (art. 31 ust. 1 pkt 3 UODO policyjne)		
jakość danych: prawidłowe i w razie potrzeby uaktualniane (art. 31 ust. 1 pkt 4 UODO policyjne)		
okres przechowywania: ograniczony nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (art. 31 ust. 1 pkt 5 UODO policyjne)		
opracowanie i wdrożenie: polityki ochrony danych osobowych (art. 31 ust. 4 UODO policyjne)		
udokumentowanie: faktycznych lub prawnych przyczyny odmowy przekazania informacji lub udostępnienia danych osobowych osobie, której dane dotyczą (art. 31. ust. 7 UODO policyjne),		
udokumentowanie: faktycznych lub prawnych przyczyny odmowy lub ograniczenia dostępu do		

danych (art. 23 ust. 4 UODO policyjne)		
udokumentowanie: odpowiednich środków technicznych oraz niezbędnych zabezpieczeń stosowanych przy przetwarzaniu danych osobowych (art. 32 ust. 3 UODO policyjne)		
jeśli administrator działa w modelu współadministrowania: czy zawarto Porozumienie? (art. 33 UODO policyjne)		
umowa o powierzeniu przetwarzania danych osobowych (w przypadku powierzania danych osobowych do przetwarzania -art. 34 UODO policyjne)		
weryfikacja danych osobowych -art. 16 ust. 1 UODO policyjne		

5.3 Środki ochrony praw i wolności osób

5.3.1 Ustalenie i uzasadnienie środków informowania osób

…

Tabela 12: Środki zapewniające realizację prawa do informacji

Środki zapewniające prawo do informacji	Implementacja	Uzasadnienie implementacji lub jej braku lub wskazanie zwolnienia z realizacji obowiązku informacyjnego
Udostępnienie informacji w związku z art. 22 ust. 1 UODO policyjnego		
Czytelne i łatwe do zrozumienia informacje (art. 22 ust. 1)		
Spełnienie warunków braku informowania osoby fizycznej w związku z treścią art. 26 ust. 1		
Prezentacja informacji w celu umożliwienie osobie wykonania przysługujących jej praw (art. 22 ust. 4 UODO policyjnego)		
Prezentacja danych kontaktowych (dane osobowe i kontaktowe do IOD)		
Zapewnienie: Prawa do uzyskania informacji o przetwarzaniu danych osobowych.		
Zapewnienie: Prawa do uzyskania informacji o przetwarzaniu danych osobowych		
Zapewnienie: Prawa dostępu do danych oraz uzyskania kopii lub wyciągu z danych.		
Zapewnienie: Prawa do uzupełnienia, uaktualnienia lub sprostowania danych osobowych.		
Zapewnienie: Prawa do usunięcia danych osobowych.		
W odniesieniu do udostępnienia danych stronom trzecim:		
- szczegółowe przedstawienie celów przekazywania danych osobom trzecim		

Środki zapewniające prawo do informacji	Implementacja	Uzasadnienie implementacji lub jej braku lub wskazanie zwolnienia z realizacji obowiązku informacyjnego
- szczegółowa prezentacja przesłanych danych osobowych		
- wskazanie tożsamości podmiotów trzecich		

5.3.2 Ustalenie i uzasadnienie środków dotyczących podmiotów przetwarzających

Tabela 13: Wykaz środków stosowanych przez podmioty przetwarzające dane

Nazwa podmiotu	Cel	Zakres	Numer umowy lub zasady zależności	Zgodność z art. 34 UODO policyjnego

5.3.3 Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej

Tabela 14: Zakres przekazywanych danych oraz adresaci*

Dane i ich lokalizacja	Polska	EU	Kraj uznany za gwarantujący równoważną ochronę jak w UE	Inne kraje	Uzasadnienie oraz sposób nadzoru (klauzule umowne, regulacje wewnętrzne, korporacyjne itp.)
-=-	-=-	-=-	-=-	-=-	-=-

* Nie dotyczy!

5.4 Ocena środków ochrony praw i wolności osób

Ocena przyjętych środków dokonywana jest przez Inspektora Ochrony Danych lub osobę wyznaczoną przez Administratora, która wypełnia poniższą tabelę. Kolejne wersje dokumentu mogą być przechowywane, jako udokumentowanie procesu zatwierdzania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, w związku z art. 37 ust. 1 UODO policyjnego.

Tabela 15: Ocena środków ochrony

Środki ochrony praw osób	Akceptacja /	Propozycje korekty środków

	możliwość udoskonalenia lub korekty	
Udostępnienie informacji, o których mowa w art. 22 ust. 1 zgodnie z wymogiem art. 22 ust. 2 (strona BIP)		
Wykonywanie praw dostępu do danych oraz uzyskania kopii lub wyciągu z danych		
Korzystanie z praw przez osobę fizyczną, której dane dotyczą		
Podmioty przetwarzające: zidentyfikowane i związane umową (lub zależnością służbową)		
Transfer danych poza UE: zgodność z obowiązkami dotyczącymi przekazywania danych poza Unię Europejską		

6 Ocena istniejących i planowanych zabezpieczeń

W niniejszym rozdziale należy ocenić istniejące, lub planowane (już przedsięwzięte) środki zabezpieczające, które mogą przybierać trzy różne formy:

1) środki dotyczące konkretnie przetwarzanych danych: szyfrowanie, anonimizacja, partycjonowanie, kontrola dostępu, identyfikowalność itd.;
2) ogólne środki bezpieczeństwa dotyczące systemu, w którym przeprowadzane jest przetwarzanie: bezpieczeństwo operacyjne, kopie zapasowe, bezpieczeństwo sprzętu itp.;
3) środki organizacyjne (zarządcze): polityka, zarządzanie projektem, zarządzanie personelem, zarządzanie incydentami i naruszeniami, relacje z osobami trzecimi itp.

Ocena przyjętych środków dokonywana jest przez Inspektora Ochrony Danych lub osobę wyznaczoną przez Administratora, która wypełnia tabele 16-20.
Kolejne wersje dokumentu stanowiącego zapis oceny ryzyka naruszenia praw i wolności osób, których dane dotyczą.

6.1 Ocena środków ochrony specyficznych dla danych osobowych

Tabela 16: Akceptacja środków ochrony danych

Środki dotyczące przetwarzanych danych	Implementacja lub uzasadnienie jej braku	Akceptacja / możliwość udoskonalenia lub korekty	Propozycje korekty środków
Szyfrowanie	Opisać środki wdrożone w celu zapewnienia poufności przechowywanych danych (w bazie danych, w plikach, kopiach zapasowych itp.), a także procedurę zarządzania kluczami szyfrowania (tworzenie, przechowywanie, zmiana w przypadku podejrzenia o przypadki ujawnienia danych itp.). Opisz zaimplementowane środki szyfrujące używane do przepływu danych (VPN, TLS itp.) w ramach czynności przetwarzania.		
Anonimizacja	Wskazać tutaj, czy wdrożono mechanizmy anonimizacji, jakie i w jakim celu.		

Partycjonowanie danych (w stosunku do pozostałej części systemu informacyjnego)	Jeśli partycjonowanie jest stosowane lub zostało zaplanowane opisać, w jaki sposób jest prowadzone, w jaki sposób działa.		
Kontrola dostępu	Opisać czy są zdefiniowane i przypisane profile użytkowników. Opisać wdrożone środki uwierzytelniania. Opisać zasady dotyczące haseł (minimalna długość, wymagane znaki, czas ważności, liczba nieudanych prób przed zablokowaniem dostępu do konta itp.)		
Śledzenie (logowanie)	Opisać, czy i jakie zdarzenia są rejestrowane i jak długo te ślady są przechowywane.		
Spójność danych	Opisać mechanizmy wdrożone w celu monitorowania integralności przetwarzanych danych, których i w jaki sposób. Opisać, które mechanizmy kontroli integralności są implementowane w przepływie danych.		
Archiwizacja	Opisać proces zarządzania archiwami (dostarczanie, przechowywanie, konsultacje itp.) w ramach właściwości. Opisać role w procesie archiwizacji (urzędy pochodzenia, strony przekazujące itp.) oraz zasady archiwizacji. Podać, czy dane mogą należeć do archiwów publicznych.		
Bezpieczeństwo dokumentów papierowych	W przypadku dokumentów papierowych zawierających dane podczas przetwarzania należy wskazać, w jaki sposób są one drukowane, przechowywane, niszczone i wymieniane.		
Inne, niewymienione wyżej środki	Opisać zasadę działania środka ochrony oraz w jaki sposób wpływa on na bezpieczeństwo		

6.2 Ocena ogólnych środków ochrony

Tabela 17: Akceptacja ogólnych środków ochrony

Ogólne środki ochrony dotyczące systemu przetwarzania danych	Implementacja lub uzasadnienie jej braku	Akceptacja / Konieczność udoskonalenia lub korekty	Propozycje korekty środków
Bezpieczeństwo oprogramowania operacyjnego	Opisać, w jaki sposób przeprowadzane są aktualizacje oprogramowania (systemy operacyjne, aplikacje itp.) oraz w jaki sposób stosowane są korekty zabezpieczeń.		
Ochrona antywirusowa	Opisać, czy oprogramowanie antywirusowe jest instalowane i aktualizowane w regularnych odstępach czasu na stacjach roboczych		
Bezpieczeństwo stacji roboczych	Opisać środki ochrony zaimplementowane na stacjach roboczych (automatyczne blokowanie, firewall, blokowanie peryferiów, itp.).		
Bezpieczeństwo witryn oraz serwisów webowych	Opisać zaimplementowane środki ochrony witryn i serwisów		
Kopie zapasowe	Opisać, w jaki sposób odbywa się zarządzane są kopiami zapasowymi oraz, czy są przechowywane w bezpiecznym miejscu.]		
Serwisowanie	Opisać, zarządzanie konserwacją sprzętu oraz, czy odbywa się na podstawie umowy.		

	Opisać, czy zdalna konserwacja aplikacji jest autoryzowana i odbywa się zgodnie z ustaleniami. Opisać sposób postępowania z wadliwym sprzętem.		
Bezpieczeństwo kanałów komputerowych (sieci)	Opisać rodzaj sieci, w której odbywa się przetwarzanie (wydzielona fizycznie, prywatna i/lub Internet). Opisać, jaka zapora, system wykrywania włamań lub inne aktywne lub pasywne urządzenia są odpowiedzialne za zapewnienie bezpieczeństwa sieci.		
Monitorowanie / nadzór	Opisać, czy zaimplementowano monitorowanie sieci lokalnej w czasie rzeczywistym i w jaki sposób. Opisać, czy monitoruje się konfigurację sprzętu i oprogramowania i w jaki sposób.		
Dostęp fizyczny	Opisać, w jaki sposób przeprowadzana jest fizyczna kontrola dostępu do pomieszczeń przetwarzania (podział na strefy, eskortowanie odwiedzających, noszenie identyfikatorów, zamknięte drzwi itp.). Opisać, jakie są procedury w przypadku włamania.		
Bezpieczeństwo sprzętu	Opisać środki fizycznego bezpieczeństwa serwerów i stacji roboczych należących do klientów (bezpieczne przechowywanie, bezpieczne kable, filtry poufności, bezpieczne usuwanie danych przed złomowaniem itp.)		
Unikanie źródeł ryzyka	Opisać, czy obszar podlega katastrofom (powódź, bliskość przemysłu chemicznego, trzęsienie ziemi lub strefa wulkaniczna itp.). Opisać, czy w pobliżu są przechowywane produkty niebezpieczne.		
Ochrona przed ryzykami niezależnymi od człowieka	Opisać środki zapobiegania, wykrywania i zwalczania pożaru. Opisać środki zapobiegające zalaniu lub podtopieniu. Opisać środki monitorowania i zapewnienia zasilania.		
Inne, niewymienione wyżej środki	Opisać zasadę działania środka ochrony oraz w jaki sposób wpływa on na bezpieczeństwo		

6.3 Ocena organizacyjnych środków ochrony

Tabela 18: Akceptacja organizacyjnych środków ochrony

Organizacyjne środki ochrony	Implementacja lub uzasadnienie jej braku	Akceptacja / Konieczność udoskonalenia lub korekty	Propozycje korekty środków
Organizacja	Opisać, czy zdefiniowano role i obowiązki w zakresie ochrony danych. Opisać, jaka osoba jest odpowiedzialna za egzekwowanie przepisów i regulacji dotyczących prywatności. Opisać, czy istnieje komitet monitorujący (lub jego odpowiednik) odpowiedzialny za wskazówki i działania następcze w zakresie ochrony prywatności.		
Polityka	Opisać, czy istnieje dokument w zakresie ochrony danych i właściwego korzystania z zasobów IT.		
Ocena ryzyka	Opisać, czy prowadzona jest ocena ryzyka naruszenia prywatności wynikająca z nowych sposobów przetwarzania danych, czy ocena ryzyka jest systematyczne, czy też nie, i jaką wybrano metodę. Opisać, czy zostało ustalone mapowanie ryzyka		

	prywatności na poziomie organizacji.		
Zarządzanie projektem	Opisać czy projektowanie i testy odbywają się na zanonimizowanych danych.		
Zarządzanie incydentami i naruszeniami	Opisać, czy incydenty informatyczne i naruszenia bezpieczeństwa podlegają udokumentowanej procedurze zarządzania.		
Zarządzanie personelem	Opisać, jakie stosowane są środki podnoszące świadomość w odniesieniu do nowych pracowników. Opisać, jakie stosowane są środki zabezpieczające, w stosunku do osób, które opuszczają pracę, a posiadały dostęp do danych.		
Relacje ze stronami trzecimi	Opisać, środki bezpieczeństwa oraz ustalenia dotyczące dostępu do danych w przypadku podmiotów przetwarzających		
Nadzór	Opisać, czy monitoruje się skuteczność i adekwatność środków ochrony prywatności.		
Inne, niewymienione wyżej środki	Opisać zasadę działania środka ochrony oraz w jaki sposób wpływa on na bezpieczeństwo		

6.4 Ocena ryzyka naruszeń bezpieczeństwa

W niniejszym rozdziale należy dokonać podsumowania oceny ryzyka dla podstawowych atrybutów informacji, pod kątem zabezpieczenia przed naruszeniami bezpieczeństwa, w ramach której należy uwzględnić najważniejsze zastosowane oraz planowane środki zabezpieczające.
Podsumowanie powinno być dokonane w oparciu o dotychczas przeprowadzone analizy oraz oceny.

Tabela 19: Akceptacja środków ochrony przeciwko naruszeniom

Organizacyjne środki ochrony	Implementacja lub uzasadnienie jej braku	Akceptacja / możliwość udoskonalenia lub korekty	Propozycje korekty środków	Ocena prawdo-podobieństwa [1 – 5]	Ocena oddziaływania [1 – 5]	Ocena skutków [1 – 25]
Nieuprawniony dostęp do danych *(naruszenie poufności)*	Osoba oceniająca musi ustalić, czy istniejące lub planowane (już podjęte) środki w wystarczającym stopniu redukują ryzyko, aby można było je zaakceptować.	Należy wskazać tutaj wszelkie dodatkowe środki, które okażą się niezbędne.				
Nieuprawniona modyfikacja danych *(naruszenie Integralności*	Osoba oceniająca musi ustalić, czy istniejące lub planowane (już podjęte) środki w wystarczającym stopniu redukują ryzyko, aby można było je zaakceptować.	Należy wskazać tutaj wszelkie dodatkowe środki, które okażą się niezbędne.				
Utrata danych *(naruszenie dostępności)*	Osoba oceniająca musi ustalić, czy istniejące lub planowane (już podjęte) środki w wystarczającym stopniu redukują ryzyko,	Należy wskazać tutaj wszelkie dodatkowe środki, które okażą się niezbędne.				

	aby można było je zaakceptować.					
Rozliczalność dostępu do danych	Osoba oceniająca musi ustalić, czy istniejące lub planowane (już podjęte) środki w wystarczającym stopniu redukują ryzyko, aby można było je zaakceptować.	Należy wskazać tutaj wszelkie dodatkowe środki, które okażą się niezbędne.				

6.5 Podsumowanie oceny ryzyka dla prywatności

UWAGA: Podsumowanie oceny dokonywane jest przez Inspektora Ochrony Danych poprzez wstawienie znaku „X" w odpowiedniej kolumnie.

Tabela 20: Podsumowanie stanu akceptacji przyjętych zabezpieczeń

Środki redukcji ryzyka	Nieakceptowalne	Do udoskonalenia	Akceptowalne
Środki zapewniające proporcjonalność i niezbędność przetwarzania			
Środki zapewnienia zgodności z zasadami przetwarzania			
powołano i określono zadania IOD (art. 46 ust. 1 i art. 38 ust. 6 UODO policyjne)			
legalność: realizacja uprawnienia lub spełnienie obowiązku wynikającego z przepisu prawa (art. 13 UODO policyjne)			
cel lub cele: - konkretne, wyraźne i prawnie uzasadnione (art. 31 ust. 1 pkt 1 i 2 UODO policyjne)			
minimalizacja danych: adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (art. 31 ust. 1 pkt 3 UODO policyjne)			
jakość danych: prawidłowe i w razie potrzeby uaktualniane (art. 31 ust. 1 pkt 4 UODO policyjne)			
okres przechowywania: ograniczony nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (art. 31 ust. 1 pkt 5 UODO policyjne)			
weryfikacja danych osobowych -art. 16 ust. 1 UODO policyjne			
Środki ochrony praw i wolności osób			
Informowanie osób, w celu umożliwienia wykonania przysługujących jej praw (rozdz. 4 UODO policyjne)			
Realizacja prawa do ograniczenia przetwarzania oraz sprzeciwu przeciwko przetwarzaniu danych			
Podmioty przetwarzające: zidentyfikowane i związane umową			
Udostępnianie danych innym organom			
Transfer danych poza UE: Zgodność z wymaganiami dotyczącymi transferu danych osobowych poza UE			

Środki ochrony specyficzne dla danych osobowych			
Szyfrowanie			
Anonimizacja			
Partycjonowanie danych (w stosunku do pozostałej części systemu informacyjnego)			
Kontrola dostępu			
Śledzenie (logowanie, rozliczalność dostępu)			
Spójność danych			
Archiwizacja			
Bezpieczeństwo dokumentów papierowych			
Inne, niewymienione wyżej środki (….)			
Ogólne środki ochrony dotyczące systemu przetwarzania danych			
Bezpieczeństwo oprogramowania operacyjnego			
Ochrona antywirusowa			
Bezpieczeństwo stacji roboczych			
Bezpieczeństwo witryn oraz serwisów webowych			
Kopie zapasowe			
Serwisowanie			
Bezpieczeństwo kanałów komputerowych (sieci)			
Monitorowanie / nadzór			
Dostęp fizyczny			
Bezpieczeństwo sprzętu			
Unikanie źródeł ryzyka			
Ochrona przed ryzykami niezależnymi od człowieka			
Inne, niewymienione wyżej środki			
Organizacyjne środki ochrony			

Organizacja			
Polityka			
Ocena ryzyka			
Zarządzanie projektem/ zmianą w systemie			
Zarządzanie incydentami i naruszeniami			
Zarządzanie personelem			
Relacje ze stronami trzecimi			
Nadzór			
Inne, niewymienione wyżej środki			

7 Weryfikacja zakresu Oceny skutków planowanych operacji

Kryteria dopuszczalnej oceny skutków dla ochrony danych

- **zapewniono systematyczny opis operacji przetwarzania (art. 37 ust. 1 pkt 1 UODO policyjnego):**
  - ☐ uwzględniono charakter, zakres, kontekst i cele przetwarzania;
  - ☐ w rejestrze kategorii czynności przetwarzania zamieszczono dane osobowe, informacje o odbiorcach i okresie przechowywania danych osobowych (art. 35);
  - ☐ przedstawiono funkcjonalny opis operacji przetwarzania;
  - ☐ zidentyfikowano zasoby, z którymi styczność mają dane osobowe (sprzęt komputerowy, oprogramowanie, sieci, osoby, opracowania lub kanały transmisji opracowań);
  - ☐ uwzględniono przestrzeganie zatwierdzonych polityk (art. 31 ust. 4);
- **przeprowadzono ocenę skutków planowanych operacji (art. 37 ust. 1):**
  - ☐ wskazano środki, których podjęcie jest planowane w celu zabezpieczenia danych osobowych (rozdział 2, art. 39), uwzględniając:
    - ☐ środki przyczyniające się do proporcjonalności i niezbędności przetwarzania,· z uwzględnieniem następujących aspektów:
      - ☐ konkretne, wyraźne i prawnie uzasadnione cele;
      - ☐ zgodność przetwarzania z prawem;
      - ☐ dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
      - ☐ ograniczony czas przechowywania;
    - ☐ środki przyczyniające się do zachowania prawa osoby fizycznej, której dane dotyczą:
      - ☐ udostępnienie informacji wskazanych w art. 22 ust. 1 (udostępnienie informacji w BIP);
      - ☐ prawo do uzyskania informacji na wniosek osoby (art. 22 ust. 4);
      - ☐ prawo dostępu do jej danych (art. 23 ust. 1);
      - ☐ prawo do sprostowania danych i prawo do ich usunięcia (art. 24 ust. 1);

- ☐ relacje z podmiotem przetwarzającym (art. 34);
- ☐ zabezpieczenia przy przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

- **<u>przeprowadzono działania w zakresie zarządzania ryzykiem naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożeń (art. 31 ust. 1):</u>**
  - ☐ przeprowadzono szacowanie i ocenę ryzyka (analizę ryzyka);
    - ☐ zidentyfikowano możliwe skutki dla praw i wolności osób fizycznych, których dane dotyczą, w przypadku zdarzeń takich jak bezprawny dostęp, niepożądane zmiany i zniknięcie danych;
    - ☐ zidentyfikowano zagrożenia, które mogłyby doprowadzić do bezprawnego dostępu, niepożądanych zmian i zniknięcia danych;
  - ☐ przeprowadzono ocenę skutków planowanych operacji przetwarzania danych,
    - ☐ w przypadku zidentyfikowania wysokiego ryzyka naruszenie praw i wolności osób fizycznych przeprowadzono konsultacje z PUODO;
- **<u>zaangażowano zainteresowane strony</u>**:
  - ☐ skonsultowano z Administratorem sposób realizacji obowiązków wynikających z treści UODO policyjnego;
  - ☐ skonsultowano się z IOD w celu uzyskania oceny środków ochrony i zaleceń lub korekty środków;
  - ☐ zobowiązano podmioty przetwarzające do należytego przetwarzania danych osobowych zgodnie z treścią art. 34 ust. 5;
- **<u>zaangażowano realizację środków organizacyjnych:</u>**
  - ☐ prowadzona jest ewidencja wniosków o nadanie uprawnień dostępu do danych (art. 41);
  - ☐ prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych (art. 42);
  - ☐ funkcjonuje procedura postępowania z naruszeniami ochrony danych osobowych oraz rejestr naruszeń ochrony danych osobowych (art. 44)