


**SPRAWOZDANIE Z OCENY SKUTKÓW  
DLA OCHRONY DANYCH  
DLA CZYNNOŚCI PRZETWARZANIA  
<nazwa czynności przetwarzania>  
(Wzór dokumentu )**

Załącznik nr 1  
do dokumentu  
Zalecenia w sprawie oceny skutków dla ochrony danych

	<b>DPIA</b>	Strona: 2 /19
---	-------------	---------------

MINISTERSTWO FINANSÓW					
<b>Dokument</b>	Sprawozdanie z oceny skutków dla ochrony danych dla czynności przetwarzania <nazwa czynności przetwarzania> (Wzór dokumentu)				
<b>Krótki opis dokumentu</b>					
<b>Właściciel dokumentu</b>	Ministerstwo Finansów				
<b>Autorzy</b>	Zespół ds. merytorycznych				
<b>Weryfikacja formalna</b>		Data		Podpis	
<b>Akceptacja</b>		Data		Podpis	
<b>Zatwierdzenie</b>		Data		Podpis	
<b>Data druku</b>		Liczba stron		22	
<b>Nazwa pliku</b>	RODO2 Zalecenia w sprawie DPIA z1 – sprawozdanie	Status dokumentu*		Z	

(\*) Status dokumentu: O – opracowywany, Z – Zatwierdzony, Z/A – Zaktualizowany i zatwierdzony, X – Odwołany

#### Historia zmian

Nr wersji	Data	Opis	Działanie (*)	Rozdziały(**)	Autor/Autorzy
1.00	20.11.2018	Pierwsza wersja dokumentu	N	W	Zespół do spraw Bezpieczeństwa i Ochrony Danych Osobowych PUESC.DO

(\*) Działanie: N-Nowy, Z-Zmiana, W-Weryfikacja


(\*\*) Rozdziały: numery rozdziałów lub W-Wszystkie

<b>Ocena skutków dla ochrony danych osobowych dla czynności przetwarzania &lt; nazwa czynności przetwarzania &gt;:</b>		
Sporządził	Data	Podpis
Zweryfikował	Data	Podpis
Zatwierdził	Data	Podpis
Inspektor Ochrony Danych  Zatwierdzam	Data	Podpis
Opinia inspektora		
Kierownik Jednostki  Zatwierdzam	Data	Podpis

1.1.1	Spis treści	
1	Wstęp .....	4
2	Opis przetwarzania.....	5
3	Aktywa.....	6
3.1	Aktywa podstawowe .....	6
3.2	Aktywa wspierające .....	6
4	Ogólna ocena ryzyka dla bezpieczeństwa informacji .....	7
5	Studium zasad przetwarzania danych osobowych .....	7
5.1	Środki zapewniające proporcjonalność i niezbędność przetwarzania .....	7
5.1.1	Legalność danych.....	7
5.1.2	Minimalizacja danych .....	7
5.1.3	Jakość danych .....	8
5.1.4	Okres przechowywania .....	8
5.2	Ocena środków w zakresie proporcjonalności i niezbędności .....	8
5.3	Środki ochrony praw i wolności osób.....	9
5.3.1	Ustalenie i uzasadnienie środków informowania osób .....	9
5.3.2	Ustalenie i uzasadnienie środków w zakresie pozyskiwania zgody.....	9
5.3.3	Ustalenie i uzasadnienie środków dostępu do danych .....	10
5.3.4	Ustalenie i uzasadnienie środków w zakresie poprawiania i usunięcia danych .....	10
5.3.5	Ustalenie i uzasadnienie środków w zakresie ograniczenia przetwarzania danych .....	11
5.3.6	Ustalenie i uzasadnienie środków dotyczących podmiotów przetwarzających .....	11
5.3.7	Ustalenie i uzasadnienie środków dotyczących transferu danych poza UE .....	12
5.4	Ocena środków ochrony praw i wolności osób.....	12
6	Ocena istniejących i planowanych zabezpieczeń .....	12
6.1	Ocena środków ochrony specyficznych dla danych osobowych .....	13
6.2	Ocena ogólnych środków ochrony.....	14
6.3	Ocena organizacyjnych środków ochrony .....	15
6.4	Ocena ryzyka naruszeń bezpieczeństwa .....	15
6.5	Podsumowanie oceny ryzyka dla prywatności.....	16
7	Weryfikacja zakresu DPIA .....	18

#### 1.1.2 Wstęp

Opisać ogólnie czego dotyczy ocena oraz jakie założenia zostały poczynione w stosunku do przedmiotu oceny.

 Ministerstwo Finansów	DPIA	Strona: 5 /19
---	------	---------------

### 1.1.3 Opis przetwarzania

Tabela 1: Opis przetwarzania danych

L.p.	Rodzaje danych	Opis
1.	Opis czynności przetwarzania	
2.	Cel przetwarzania, podstawa prawna	1) 2)
3.	Podmioty biorące udział w przetwarzaniu (Interesariusze przetwarzania)	1) 2)
4.	Administrator danych	
5.	Podmioty przetwarzające	1) 2)
6.	Systemy wspierające przetwarzanie	1) 2)
7.	Umowy powierzenia przetwarzania danych osobowych (nr umowy, z dnia, pomiędzy, na okres, w zakresie).	Np.: Umowa powierzenia przetwarzania danych osobowych: - Nr xx/RRRR (XX0000-ILGW-xxx-xxx.RRRR) z dnia DD.MMM.RRRR r. zawarta z ... , - Nr 18/2016 (XX0000-ILGW.xxx xxx.RRRR) z dnia DD.MMM.RRRR r. zawarta z ...

Tabela 2: Standardy dotyczące przetwarzania danych osobowych

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

Tabela 3 - Przesłanki wysokiego ryzyka dla praw i wolności osób

l. p.	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 skalę miejsc dostępnych publicznie wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdują się w monitorowanej przestrzeni.		

l. p.	Przesłanki wysokiego ryzyka dla praw i wolności osób	Uzasadnienie	Opis
4.	Przetwarzanie szczególnych kategorii danych osobowych i dotyczących wyroków skazujących i czynów zabronionych (danych wrażliwych wg opinii WP 29)		
5.	Dane przetwarzane na dużą skalę, gdzie pojęcie dużej skali dotyczy: <ul style="list-style-type: none"> <li>• liczby osób, których dane są przetwarzane,</li> <li>• zakresu przetwarzania,</li> <li>• okresu przechowywania danych oraz</li> <li>• geograficznego zakresu przetwarzania</li> </ul>		
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		

1.1.4 Aktywa

1.1.5 Aktywa podstawowe

Tabela 4: Proces - aktywa podstawowe

Nazwa procesu	Rodzaje danych	Odbiorcy danych	Okres retencji danych

1.1.6 Aktywa wspierające

Tabela 5: Identyfikacja aktywów wspierających

Przetwarzanie danych	Szczegółowy opis przetwarzania	Aktywa wspierające przetwarzanie
Gromadzenie		
Użycie		
Transfer		
Retencja		
Niszczenie		

#### 1.1.7 Ogólna ocena ryzyka dla bezpieczeństwa informacji

Ocena skutków dla praw, wolności i prywatności podmiotów danych musi być poprzedzona ogólną oceną ryzyka dla bezpieczeństwa informacji.

Zalecenia dotyczące trybu i sposobu oraz zasady przeprowadzenia ogólnej oceny ryzyka dla bezpieczeństwa informacji przedstawiono w Rozdziale 6.2 „Analiza ryzyka dla bezpieczeństwa danych osobowych przetwarzanych z wykorzystaniem systemu informatycznego” dokumentu *Zalecenia w sprawie dokonywania oceny skutków dla ochrony danych (Data Protection Impact Assessment - DPIA)*.

#### 1.1.8 Studium zasad przetwarzania danych osobowych

#### 1.1.9 Środki zapewniające proporcjonalność i niezbędność przetwarzania

Tabela 6: Wyjaśnienie i uzasadnienie celów przetwarzania

l. p.	Cele przetwarzania	Uzasadnienie
1.		
2		
3		

#### 1.1.10 Legalność danych

Tabela 7: Wyjaśnienie i uzasadnienie podstawy prawnej

Podstawa prawna przetwarzania	Dotyczy (TAK / NIE)	Uzasadnienie
osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów		
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		

#### 1.1.11 Minimalizacja danych

 <b>Ministerstwo Finansów</b>	<b>DPIA</b>	Strona: 8 /19
---	-------------	---------------

Tabela 8: Wyjaśnienie i uzasadnienie minimalizacji danych

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

1.1.12 Jakość danych

Tabela 9: Środki zapewnienia jakości danych

Środki zapewniające jakość danych	Uzasadnienie

1.1.13 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			

1.1.14 Ocena środków w zakresie proporcjonalności i niezbędności

Ocena przyjętych środków dokonywana jest przez Inspektora Ochrony Danych, który wypełnia tabelę 11. Kolejne wersje dokumentu stanowiącego zapis oceny ryzyka dla prywatności mogą być przechowywane jako dokumentacja procesu zatwierdzania DPIA.

Tabela 11: Ocena środków ochrony

Środki zapewnienia zgodności z zasadami przetwarzania	Akceptacja / możliwość (udoskonalenia) korekty	Proponowane korekty środków
cel lub cele: - konkretne, wyraźne i prawnie uzasadnione (art. 5.1 b RODO)		
legalność: zgodność przetwarzania z prawem, zakaz nadużywania (art. 6 RODO)		
minimalizacja danych: adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (art. 5 c RODO)		
jakość danych: prawidłowe i w razie potrzeby uaktualniane (art. 5 d RODO)		
okres przechowywania: ograniczony nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (art. 5 e RODO)		



1.1.15 Środki ochrony praw i wolności osób

1.1.16 Ustalenie i uzasadnienie środków informowania osób

Jeżeli korzystamy ze zwolnienia z obowiązku informacyjnego, o których mowa w art. 12, 13 i 14 RODO należy uzasadnić korzystanie z tego zwolnienia.

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
Prezentacja warunków użytkowania / poufności		
Łatwość dostępu do warunków korzystania / poufności		
Czytelne i łatwe do zrozumienia warunki		
Istnienie klauzul właściwych dla urzędu		
Szczegółowe przedstawienie celów związanych z przetwarzaniem danych (określone cele, porównania danych (przesłanka 6) itp.)		
Szczegółowa prezentacja zebranych danych osobowych		
Prezentacja jakiegokolwiek dostępu do identyfikatorów urzędu, smartfona / tabletu lub komputera, określając, czy te identyfikatory są przekazywane stronom trzecim		
Prezentacja praw użytkownika (wycofanie zgody, usunięcie danych itp.)		
Informacje na temat metody bezpiecznego przechowywania danych, szczególnie w przypadku pozyskiwania		
Ustalenia dotyczące kontaktu z firmą (dane osobowe i kontaktowe) dotyczące kwestii poufności		
W stosownych przypadkach, informacje dla użytkownika o wszelkich zmianach dotyczących zgromadzonych danych, celach i klauzulach poufności		
W odniesieniu do przekazywania danych stronom trzecim:		
- szczegółowe przedstawienie celów przekazywania danych osobom trzecim		
- szczegółowa prezentacja przesłanych danych osobowych		
- wskazanie tożsamości podmiotów trzecich		

1.1.17 Ustalenie i uzasadnienie środków w zakresie pozyskiwania zgody

Tabela 13: Środki zapewniające zgodę na przetwarzanie danych

Środki w zakresie pozyskiwania zgody	Implementacja	Uzasadnienie implementacji lub jej braku
Wyrażna zgoda podczas rejestracji lub gromadzenia danych		
Zgoda podzielona na segmenty według kategorii danych lub typu przetwarzania		
Wyrażna zgoda przed udostępnieniem danych innym użytkownikom		
Zgoda przedstawiona w zrozumiałej i łatwo dostępnej formie, przy użyciu jasnego i prostego języka dostosowanego do docelowego użytkownika (w szczególności dla dzieci)		
Uzyskanie zgody rodziców dla osoby niepełnoletniej poniżej 13 roku życia		
W przypadku nowego użytkownika należy ponownie uzyskać zgodę		
Po długim okresie braku aktywności użytkownik musi zostać poproszony o potwierdzenie swojej zgody		
W przypadku gdy użytkownik wyraził zgodę na przetwarzanie danych specjalnych (np. lokalizacja), interfejs użytkownika wyraźnie wskazuje, że wspomniane przetwarzanie ma miejsce (ikona, lampka itp.)		
W przypadku zmiany przez użytkownika urządzenia, smartfona lub komputera, reinstalacji aplikacji mobilnej lub usunięcia plików cookie, ustawienia związane z wyrażoną zgodą są zachowywane		

#### 1.1.18 Ustalenie i uzasadnienie środków dostępu do danych


Tabela 14: Środki w zakresie prawa dostępu do danych

Środki w zakresie zapewnienia dostępu do danych	Dane wewnętrzne	Dane zewnętrzne	Uzasadnienie
Możliwość uzyskania dostępu do wszystkich danych osobowych użytkownika za pośrednictwem ogólnodostępnych interfejsów			
Możliwość bezpiecznego sprawdzenia śladów użytkownika dotyczących użytkownika			
Możliwość pobrania archiwum wszystkich danych osobowych związanych z użytkownikiem			

#### 1.1.19 Ustalenie i uzasadnienie środków w zakresie poprawiania i usunięcia danych

Tabela 15: Środki w zakresie prawa do poprawiania i usunięcia danych

Środki w zakresie zapewnienia prawa do poprawiania i usunięcia danych	Dane wewnętrzne	Dane zewnętrzne	Uzasadnienie
Możliwość poprawiania danych osobowych			

	<b>DPIA</b>	Strona: 11 /19
---	-------------	----------------

Możliwość usunięcia danych osobowych			
Wskazanie danych osobowych, które mimo to będą przechowywane (wymagania techniczne, zobowiązania prawne itp.)			
Wdrażanie prawa do bycia zapomnianym w stosunku do nieletnich			
Jasne wskazania i proste kroki do usuwania danych przed złomowaniem urządzenia			
Porada dotycząca resetowania urządzenia przed jego sprzedażą			
Możliwość kasowania danych w przypadku kradzieży urządzenia			

#### 1.1.20 Ustalenie i uzasadnienie środków w zakresie ograniczenia przetwarzania danych

Tabela 16: Środki w zakresie prawa do ograniczenia przetwarzania danych

Środki w zakresie zapewnienia prawa do poprawiania i usunięcia danych	Dane wewnętrzne	Dane zewnętrzne	Uzasadnienie
Istnienie ustawień "Prywatności"			
Zaproszenie do zmiany ustawień domyślnych			
Ustawienia "Prywatności" dostępne podczas rejestracji			
Ustawienia "Prywatności" dostępne po rejestracji			
Istnienie systemu kontroli rodzicielskiej dla dzieci poniżej 16 roku życia			
Zgodność w zakresie śledzenia (pliki cookie, reklama itp.)			
Wykluczenie dzieci poniżej 16 roku życia z profilowania automatycznego			
Skuteczne wyłączenie przetwarzania danych użytkownika w przypadku wycofania zgody			

#### 1.1.21 Ustalenie i uzasadnienie środków dotyczących podmiotów przetwarzających

Tabela 17: Wykaz środków stosowanych przez podmioty przetwarzające dane

Nazwa podmiotu	Cel	Zakres	Numer umowy lub zasady zależności	Zgodność z art. 28


#### 1.1.22 Ustalenie i uzasadnienie środków dotyczących transferu danych poza UE

Tabela 18: Środki stosowane przy transferze danych poza UE

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

#### 1.1.23 Ocena środków ochrony praw i wolności osób

Ocena przyjętych środków dokonywana jest przez Inspektora Ochrony Danych, który wypełnia tabelę 23. Kolejne wersje dokumentu stanowiącego zapis oceny ryzyka dla prywatności mogą być przechowywane jako dokumentacja procesu zatwierdzania DPIA.

Tabela 19: Ocena środków ochrony

Środki ochrony praw osób	Akceptacja / możliwość udoskonalenia lub korekty	Proponowane korekty środków
Informowanie osób, których dane dotyczą (uczciwe i przejrzyste przetwarzanie)		
Pozyskanie zgody		
Wykonywanie praw dostępu i przenoszenia danych		
Wykonywanie praw do sprostowania i usunięcia		
Korzystanie z prawa do ograniczenia przetwarzania i sprzeciwu		
Podmioty przetwarzające: zidentyfikowane i związane umową (lub zależnością służbową)		
Transfer danych poza UE: zgodność z obowiązkami dotyczącymi przekazywania danych poza Unię Europejską		

#### 1.1.24 Ocena istniejących i planowanych zabezpieczeń

W niniejszym rozdziale należy ocenić istniejące, lub planowane (już podjęte) 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, który wypełnia tabele 24-26. Kolejne wersje dokumentu stanowiącego zapis oceny ryzyka dla prywatności mogą być przechowywane jako dokumentacja procesu zatwierdzania DPIA.

#### 1.1.25 Ocena środków ochrony specyficznych dla danych osobowych

Tabela 20: 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 rolę 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		

#### 1.1.26 Ocena ogólnych środków ochrony

Tabela 21: 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 zarządzanie 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 zaporą, 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		

### 1.1.27 Ocena organizacyjnych środków ochrony

Tabela 22: Akceptacja organizacyjnych środków ochrony

Organizacyjne środki ochrony	Implementacja lub uzasadnienie jej braku	Akceptacja / Konieczność udoskonalenia lub korekty	Proponowane 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 systematyczna, 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		

### 1.1.28 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 uwzględnić najważniejsze zastosowane oraz planowane środki zabezpieczające.

Podsumowanie ma być dokonane w oparciu o analizę „ogólną” sporządzoną według wytycznych zawartych w dokumencie *Zalecenia w sprawie dokonywania oceny skutków dla ochrony danych (Data Protection Impact Assessment - DPIA)* i zawartą w dokumencie *Sprawozdanie z oceny ryzyka dla bezpieczeństwa danych osobowych przetwarzanych z wykorzystaniem systemu informatycznego* *<nazwa systemu informatycznego>* sporządzonego zgodnie z wzorem dokumentu stanowiącym załącznik nr 5 do dokumentu *Zalecenia w sprawie dokonywania oceny skutków dla ochrony danych (Data Protection Impact Assessment - DPIA)*.

Tabela 23: Akceptacja środków ochrony przeciwko naruszeniom

Organizacyjne środki ochrony	Implementacja lub uzasadnienie jej braku	Akceptacja / możliwość udoskonalenia lub korekty	Propozycje korekty środków	Ocena prawdopodobieństwa [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, aby można było je zaakceptować.	Należy wskazać tutaj wszelkie dodatkowe środki, które okażą się niezbędne.				
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.				

#### 1.1.29 Podsumowanie oceny ryzyka dla prywatności


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

Tabela 24: Podsumowanie stanu akceptacji przyjętych zabezpieczeń

Środki redukcji ryzyka	Nieakceptowalne	Do udoskonalenia	Akceptowalne
Środki zapewniające proporcjonalność i niezbędność przetwarzania			
<b>Środki zapewnienia zgodności z zasadami przetwarzania</b>			
cel lub cele: - konkretne, wyraźne i prawnie uzasadnione (art. 5.1 b RODO)			
legalność: zgodność przetwarzania z prawem, zakaz nadużywania (art. 6 RODO)			
minimalizacja danych: adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (art. 5 c RODO)			
jakość danych: prawidłowe i w razie potrzeby uaktualniane (art. 5 d RODO)			
okres przechowywania: ograniczony nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (art. 5 e RODO)			



Środki ochrony praw i wolności osób			
Informowanie osób, których dane dotyczą (uczciwe i przejrzyste)			
Pozyskiwanie zgody			
Realizacja prawa do dostępu i przenoszenia danych			
Realizacja prawa do poprawiania i usuwania danych			
Realizacja prawa do ograniczenia przetwarzania oraz sprzeciwu przeciwko przetwarzaniu danych			
Podmioty przetwarzające: zidentyfikowane i związane umową			
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			


	DPIA	Strona: 18 /19
---	------	----------------

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			
Zarządzanie incydentami i naruszeniami			
Zarządzanie personelem			
Relacje ze stronami trzecimi			
Nadzór			
Inne, niewymienione wyżej środki			

#### 1.1.30 Weryfikacja zakresu DPIA

##### Kryteria dopuszczalnej oceny skutków dla ochrony danych

- **zapewniono systematyczny opis operacji przetwarzania (art. 35 ust. 7 lit. a)):**
- uwzględniono charakter, zakres, kontekst i cele przetwarzania (motyw 90);
  - w rejestrze zamieszczono dane osobowe, informacje o odbiorcach i okresie przechowywania danych osobowych;
  - przedstawiono funkcjonalny opis operacji przetwarzania;
  - zidentyfikowano zasoby, z którymi styczność mają dane osobowe (sprzęt komputerowy, oprogramowanie, sieci, osoby, opracowania lub kanały transmisji opracowań);

	<p style="text-align: center;"><b>DPIA</b></p>	<p style="text-align: right;">Strona: 19 /19</p>
---	--	--

- uwzględniono przestrzeganie zatwierdzonych kodeksów postępowania (art. 35 ust. 8);
- **oceniono niezbędność oraz proporcjonalność (art. 35 ust. 7 lit. b)):**
  - wskazano środki, których podjęcie jest planowane w celu zapewnienia przestrzegania rozporządzenia (art. 35 ust. 7 lit. d) i motyw 90), uwzględniając:
    - środki przyczyniające się do proporcjonalności i niezbędności przetwarzania, z uwzględnieniem następujących aspektów:
      - konkretne, wyraźne i prawnie uzasadnione cele (art. 5 ust. 1 lit. b));
      - zgodność przetwarzania z prawem (art. 6);
      - dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (art. 5 ust. 1 lit. c));
      - ograniczony czas przechowywania (art. 5 ust. 1 lit. e));
    - środki przyczyniające się do zachowania praw osób, których dane dotyczą:
      - poinformowanie osoby, której dane dotyczą (art. 12, 13 i 14);
      - prawo dostępu i prawo do przenoszenia danych (art. 15 i 20);
      - prawo do sprostowania i do usunięcia danych (art. 16, 17 i 19);
      - prawo do sprzeciwu i prawo do ograniczenia przetwarzania (art. 18, 19 i 21);
    - relacje z podmiotem przetwarzającym (art. 28);
    - zabezpieczenia przy międzynarodowym przekazywaniu danych (rozdział V);
    - uprzednie konsultacje (art. 36);
- **przeprowadzono działania w zakresie zarządzania ryzykiem naruszenia praw i wolności osób, których dane dotyczą (art. 35 ust. 7 lit. c)):**
  - uwzględniono źródło, charakter, specyfikę i powagę ryzyka (por. motyw 84), czy konkretniej, w przypadku każdego rodzaju ryzyka (bezprawnego dostępu, niepożądaną zmiany i zniknięcia danych), z punktu widzenia osób, których dane dotyczą:
    - uwzględniono źródła ryzyka (motyw 90);
    - zidentyfikowano możliwe skutki dla praw i wolności osób, 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;
    - oszacowano prawdopodobieństwo i powagę (motyw 90);
  - określono środki, których podjęcie jest planowane w celu zaradzenia ryzyku (art. 35 ust. 7 lit. d) i motyw 90);
- **zaangażowano zainteresowane strony:**
  - skonsultowano się z inspektorem ochrony danych w celu uzyskania zalecenia (art. 35 ust. 2);
  - w stosownych przypadkach zasięgnięto opinii osób, których dane dotyczą, lub ich przedstawicieli (art. 35 ust. 9).