Załącznik do zarządzenia Nr 16
Dyrektora Generalnego
z dnia 12 kwietnia 2023 r.

Polityka zarządzania ryzykiem

w Lubuskim Urzędzie Wojewódzkim

LUBUSKI
URZĄD WOJEWODZKI

Spis treści

Słownik pojęć

Ryzyko – możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów i zadań Lubuskiego Urzędu Wojewódzkiego w Gorzowie Wlkp. Ryzyko może mieć charakter negatywnego zagrożenia lub pozytywnej możliwości. Na potrzeby zarządzania ryzkiem naruszania praw i wolności osób fizycznych, o różnym prawdopodobieństwie i wadze zagrożenia „ryzyko" jest scenariuszem opisującym zdarzenie i jego konsekwencje, oszacowanym pod względem powagi i prawdopodobieństwa ryzyka[1].

Ryzyko nieodłączne – ryzyko przed wprowadzeniem mechanizmów kontrolnych. Narażenie spowodowane określonym ryzykiem przed podjęciem jakichkolwiek działań w celu zarządzania nim.

Ryzyko rezydualne – ryzyko po wprowadzeniu mechanizmów kontrolnych. Narażenie spowodowane określonym ryzykiem po podjęciu działania w celu zarządzania nim i przyjęciu założenia, że działanie to jest skuteczne.

Mechanizm kontrolny – element systemu zarządzania, zasady określone przez przepisy prawa lub uregulowania wewnętrzne mające ograniczyć prawdopodobieństwo wystąpienia ryzyka lub ograniczyć ryzyko.

Akceptowalny poziom ryzyka (apetyt na ryzyko) – poziom ryzyka, który Urząd może ponieść w razie jego wystąpienia. Przy wyznaczaniu akceptowalnego poziomu ryzyka uwzględnienia się sytuację Urzędu, wielkości kosztów ograniczenia danego ryzyka oraz możliwości wpływu na ryzyko.

Właściciel ryzyka – osoba odpowiedzialna za zarządzanie ryzykiem, mająca kompetencje do podjęcia działań zarządczych w stosunku do obszaru, którym zarządza.

Zarządzanie ryzykiem – ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy.

Zespół ds. zarządzania ryzykiem – zespół powołany w celu koordynowania działań związanych z zarządzaniem ryzykiem.

[1] Wytyczne dotyczące oceny skutków dla ochrony danych DPIA oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679, 17/EN, WP 248 rev.01, Ostatnio zmienione i przyjęte w dniu 4 października 2017 r.

Wprowadzenie

Niniejszy dokument opisuje ogół działań dotyczących zarządzania ryzykiem w jednostce, które mają zapewnić realizację celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy. Zapisy Polityki zarządzania ryzykiem opierają się na Strategii rozwoju Lubuskiego Urzędu Wojewódzkiego w Gorzowie Wlkp. oraz wskazują kierunki działań, które umożliwią osiągnięcie wskazanych celów strategicznych, przy jak najlepszym wykorzystaniu potencjału i posiadanych zasobów.

Celem zarządzania ryzykiem w odniesieniu do postawionych celów i zadań Urzędu jest:

- maksymalne ograniczenie zidentyfikowanego ryzyka negatywnie wpływającego na realizację celów i zadań Urzędu,
- maksymalne wykorzystanie możliwości i szans stojących przed Urzędem oraz ograniczenie ryzyka utraty szans,
- usprawnienie efektywności zarządzania Urzędem poprzez utworzenie właściwego ładu organizacyjnego,
- efektywne wykorzystanie zasobów finansowych, ludzkich, materialnych oraz zapobieganie stratom finansowym,
- poprawa jakości świadczenia usług.

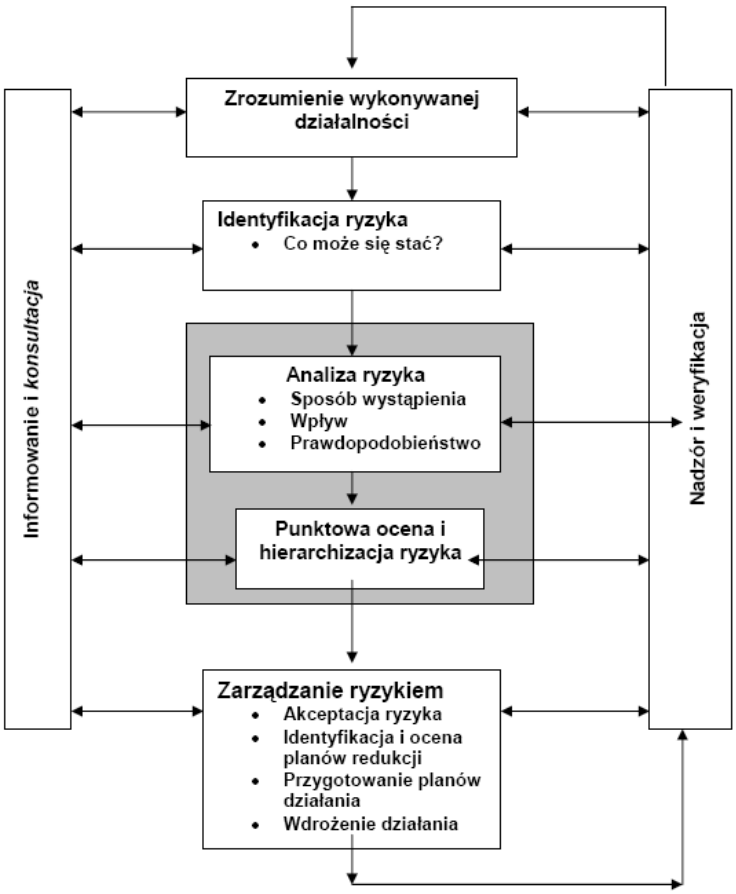
Proces zarządzania ryzykiem składa z następujących etapów:

1. identyfikacji,
2. analizy,
3. oceny punktowej,
4. hierarchizacji,
5. zarządzania.

Polityka zarządzania ryzykiem w Urzędzie jest zdefiniowana dla następujących poziomów:

a. celów strategicznych – określonych w Strategii rozwoju Lubuskiego Urzędu Wojewódzkiego w Gorzowie Wlkp.,
b. celów cząstkowych – określonych w Wieloletnim Planie Finansowym Państwa, budżecie zdaniowym na poziomie funkcji, zadań i podzadań oraz Rocznym Programie Działania Urzędu,
c. celów operacyjnych – określonych w budżecie zdaniowym na poziomie działań, a jeżeli jest to niemożliwe, na podstawie Regulaminu organizacyjnego Urzędu.

Poniższy schemat przedstawia powiązania pomiędzy etapami procesu zarządzania ryzykiem w Urzędzie.



Na każdym z etapów procesu zarządzania ryzykiem prowadzone są działania informacyjne oraz konsultacje mające na celu zapewnienie, że pracownicy urzędu rozumieją wykonywaną działalność. Pracownicy Urzędu powinni rozumieć działalność, którą wykonują.

Polityka zarządzania ryzykiem ma zastosowanie do wszystkich komórek organizacyjnych Urzędu oraz do wszystkich pracowników Urzędu. Obowiązków i zadań w zakresie zarządzania ryzykiem nie można ograniczyć do jednej komórki organizacyjnej Urzędu.

Ocena systemu zarządzania ryzykiem w Urzędzie, a także czynności doradcze dokonywane przez audyt wewnętrzny wspierają Kierownika Urzędu w realizacji celów i zadań jednostki.

Kierownik Urzędu wyznacza akceptowalny poziom ryzyka, który Urząd może ponieść w razie jego wystąpienia. Przy wyznaczaniu akceptowalnego poziomu ryzyka uwzględnienia się sytuację Urzędu, wielkości kosztów ograniczenia danego ryzyka oraz możliwości wpływu na ryzyko.

1. Identyfikacja ryzyka

Identyfikacja ryzyka jest pierwszym etapem procesu zarządzania ryzykiem. Identyfikacja i przegląd ryzyka dokonywane są corocznie. Proces identyfikacji oraz przeglądu ryzyka przeprowadzany jest przez Zespół, który na podstawie profesjonalnego osądu tworzy katalog ryzyk dla Urzędu.

Zadaniem Zespołu jest przeprowadzenie analizy wszystkich procesów przebiegających w Urzędzie, które zmierzają do realizacji postawionych przed Urzędem celów i zadań oraz zidentyfikowaniem związanego z nimi ryzyka. Zespół dokonuje identyfikacji ryzyka stosując metodę „Burzy mózgów".

Katalog zidentyfikowanych ryzyk, na które narażony jest Urząd przy realizacji celów i zadań może być uzupełniony o ryzyka zgłaszane przez pracowników Urzędu.

2. Analiza ryzyka

Zidentyfikowane ryzyka poddawane są analizie. W procesie zarządzania ryzkiem naruszania praw i wolności osób fizycznych właściciel ryzyka dodatkowo wskazuje czynność/czynności i/lub kategorię/kategorie przetwarzania danych osobowych.

Dla każdego zidentyfikowanego ryzyka należy określić: przyczyny ryzyka oraz oddziaływanie (wpływ) ryzyka na organizację w razie jego wystąpienia.

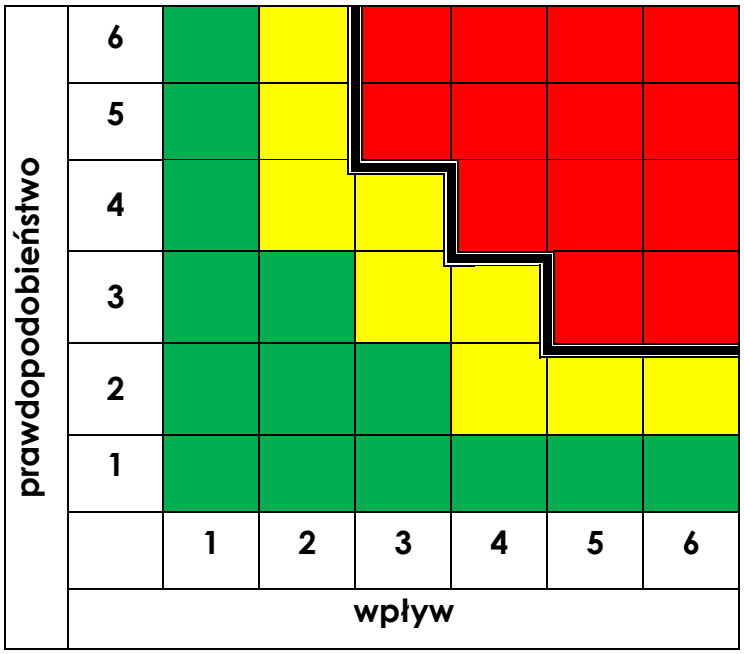
Analiza ryzyka dokonywana jest przez Zespół na podstawie wypełnionego przez pracowników Urzędu formularza ankietowego. Pracownicy Urzędu wypełniają kwestionariusz udzielając odpowiedzi „Tak" lub „Nie" na pytania, które służą do ustalenia prawdopodobieństwa wystąpienia danego ryzyka. Kombinacja udzielonych przez pracowników odpowiedzi na pytania do poszczególnych ryzyk pozwala określić prawdopodobieństwo wystąpienia danego ryzyka. Prawdopodobieństwo wystąpienia ryzyka określane jest w stosunku do każdego zadania określonego w określonych w budżecie zdaniowym na poziomie działań lub wskazanego przez Wydział/Biuro na podstawie regulaminu organizacyjnego. Za pomocą kwestionariusza określa się również wpływ ryzyka na osiągnięcie celu w stosunku do każdego zadania.

3. Ocena punktowa ryzyka

Ocena punktowa ryzyka dokonywana jest przez Zespół. Ocena ryzyka dokonywana jest przy zapewnieniu ustrukturyzowanego procesu uwzględniającego zarówno prawdopodobieństwo jego wystąpienia, jak i jego oddziaływanie. Dla poszczególnych kategorii wpływu ustalone zostały wagi. Dokonując oceny punktowej ryzyka brana jest pod uwagę suma iloczynów poszczególnych kategorii wpływów i wag im przypisanych.

W procesie zarządzania ryzykiem naruszenia bezpieczeństwa informacji oraz procesie zarządzania ryzkiem naruszania praw i wolności osób fizycznych punktowa ocena ryzyka składa się dodatkowo z oceny skuteczności stosowanych zabezpieczeń.

Proces oceny ryzyka jest dokumentowany oraz monitorowany. Skalę analityczną stanowi macierz „6x6". Matrycę ryzyka tworzy sześciopunktowa skala dla prawdopodobieństwa wystąpienia ryzyka oraz sześciopunktowa skala dla wpływu ryzyka.



Dyrektor Generalny Lubuskiego Urzędu Wojewódzkiego w Gorzowie Wlkp., wskazuje akceptowalny poziom ryzyka dla Urzędu. Wartość ryzyka akceptowalnego została określona na poziomie 12.

Ryzyko mieszczące się w przedziale wartości od <1 do 6) (kolor zielony) nie wymaga podjęcia działań, a jego poziom nie zagraża realizacji celów i zadań postawionych przed LUW.

Ryzyko mieszczące się w przedziale wartości od <6 do 12) (kolor żółty) wymaga ciągłego monitorowania.

Ryzyko, którego poziom przekroczył wartość 5 tj. mieszczące się w przedziale wartości od <12 do 36> (kolor czerwony) wymaga podjęcia działań zmierzających do jego ograniczenia.

Prawdopodobieństwo oraz wpływ wystąpienia danego zdarzenia zostały określone przez właścicieli ryzyka (realizatorów zadań). Kombinacja udzielonych przez właścicieli ryzyka odpowiedzi dała informację na temat prawdopodobieństwa wystąpienia danego ryzyka przy realizacji zadania. Skalę dla prawdopodobieństwa wystąpienia ryzyka określono w następujący sposób:

Prawdopodobieństwo	wartość	opis
	1	zdecydowanie się nie zdarzy
	2	raczej się nie zdarzy
	3	możliwe, że się nie zdarzy
	4	możliwe, że się zdarzy
	5	raczej się zdarzy
	6	zdecydowanie się zdarzy

Skalę dla wpływu ryzyka określono w następujący sposób:

wpływ	wartość	opis
	1	nieodczuwalne
	2	nieznaczne
	3	małe
	4	średnie
	5	poważne
	6	katastrofalne

Co do zasady, w procesie zarządzania ryzkiem naruszania praw i wolności osób fizycznych uznaje się, że skutkom materializacji ryzyka należy przypisać wartość odpowiadającą najwyższemu stopniowi wpływu, jeżeli przetwarzanie spełniające przynajmniej dwa ze wskazanych poniżej kryteriów. Kryteria dla wpływu na ryzyko naruszenia praw i wolności osób fizycznych określono w na stepujący sposób.

Ocena wpływu materializacji ryzyka na osoby, których dane dotyczą
1. Materializacja ryzyka może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną
2. Osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi
3. Przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa
4. Oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych
5. Przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci

6. Przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą

Formularz ankietowy zawiera również część, w której właściciel ryzyka szacuje wpływ wystąpienia danego zdarzenia przy realizacji zadania (nie dotyczy zarządzania ryzykiem naruszenia bezpieczeństwa informacji oraz procesie zarządzania ryzkiem naruszania praw i wolności osób fizycznych). Wpływ wystąpienia zdarzenia jest określany w podziale na przyjęte kategorie, które determinowane są skutkami takimi jak: finansowe, organizacyjne, zdrowie i bezpieczeństwo, reputacja. Wagi poszczególnych kategorii wpływów określono w następujący sposób:

kategoria wpływu	waga	opis
	0,24	finansowy
	0,19	organizacyjny
	0,42	ochrona zdrowia i bezpieczeństwa
	0,15	reputacja

Skala skuteczności stosowanych zabezpieczeń w procesie zarządzania ryzykiem naruszenia bezpieczeństwa informacji oraz procesie zarządzania ryzkiem naruszania praw i wolności osób fizycznych.

skuteczność	wartość	opis
	1	Brak zidentyfikowanych obszarów niechronionych
	2	Nieistotne zidentyfikowane obszary niechronione
	3	Nieliczne zidentyfikowane obszary niechronione
	4	Chronione wybrane obszary
	5	Istotne lub liczne obszary niechronione
	6	Brak zabezpieczeń

Ocena punktowa ryzyka wykonywana jest według wzoru:

wartość ryzyka = prawdopodobieństwo x wpływ

Ocena punktowa ryzyka w procesie zarządzania ryzykiem naruszenia bezpieczeństwa informacji oraz procesie zarządzania ryzkiem naruszania praw i wolności osób fizycznych wykonywana jest według wzoru:

wartość ryzyka = (prawdopodobieństwo x wpływ)

/ocena skuteczności zabezpieczeń

4. Pogłębiona analiza ryzyka

Jeżeli wyniki szczegółowe w poszczególnych katalogach zidentyfikowanych ryzyk przekraczają akceptowalny poziom 12, właściciele ryzyka przechodzą do drugiego etapu badania, w którym wypełniają pogłębione ankiety. Arkusze te pozwalają doprecyzować zagrożenia i wskazać czynniki wpływające na ich materializację. Zobowiązują również ankietowanych do wskazania podjętych dotychczas działań zaradczych i zaproponowania dalszych działań, które zminimalizują ryzyko w poszczególnych katalogach.

5. Hierarchizacja ryzyka

Po przeprowadzeniu oceny punktowej ryzyka przez Zespół, przeprowadzana jest hierarchizacja ryzyka polegająca na uporządkowaniu zadań według wartości ryzyka określonej podczas oceny. Wartości ryzyka rezydualnego uszeregowano od wartości najwyższej do najniższej z podziałem na wydziały/biura, oddziały/samodzielne stanowiska oraz zadania.

6. Zarządzanie ryzykiem

Głównymi zadaniami etapu realizowanymi w ramach zarządzania zidentyfikowanym ryzykiem są akceptacja ryzyka, identyfikacja i ocena planów redukcji ryzyka, przygotowanie odpowiednich planów działania oraz ich wdrożenie. Proces zarządzania ryzykiem obejmuje:

1. Podjęcie działań w celu zmniejszenia ryzyka, gdy zachodzi taka potrzeba w stosunku do ryzyka, którego wartość przekracza poziom wskazany jako dopuszczalny. Należy podjąć działania, by zmniejszyć ryzyko.
2. Zapewnienie skuteczności funkcjonujących mechanizmów kontroli, poprzez przegląd skuteczności mechanizmów (różnica pomiędzy ryzykiem nieodłącznym i rezydualnym).
3. Monitoring i raportowanie ryzyka, który obejmuje wykonywanie przez Zespół przeglądu w celu określenia, czy ryzyko uległo zmianie, sprawdzenie czy punktowa ocena ryzyka jest wciąż odpowiednia oraz monitorowanie rozwoju uzgodnionych działań w zakresie zarządzania ryzykiem.

Zarządzanie ryzykiem w Lubuskim Urzędzie Wojewódzkim w Gorzowie Wlkp. ma na celu:

- zwiększenie prawdopodobieństwa realizacji zadań i osiągania celów,
- zapewnienie odpowiednich mechanizmów kontroli wewnętrznej,
- zapewnienie Dyrektorowi Generalnemu Urzędu wczesnej informacji o zagrożeniach dla realizacji wyznaczonych celów i zadań.

Reakcja na ryzyko może przybierać różne formy, m.in. zmniejszenie ryzyka poprzez, np.: zaprojektowanie i wdrożenie mechanizmów kontroli; przeniesienia ryzyk – wykupienie ubezpieczenia; akceptację istniejącego ryzyka.

Ryzyko przekraczające akceptowany poziom, wymaga ustalenia i podjęcia działań przez właściciela ryzyka ograniczających je do akceptowanego poziomu poprzez zmniejszenie prawdopodobieństwa lub wpływu jego wystąpienia.

Jeżeli ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą wskaże, że przetwarzanie powodowałoby wysokie ryzyko, to przed rozpoczęciem przetwarzania administrator konsultuje się z Prezesem Urzędu Ochrony Danych Osobowych.

W celu określenia metody przeciwdziałania ryzyku należy przeanalizować:

- przyczyny (źródła) ryzyka i możliwe scenariusze rozwoju wydarzeń,
- istniejące mechanizmy kontroli stosowane w celu ograniczenia lub uniknięcia ryzyka,
- skuteczność istniejących mechanizmów kontroli, tj. zakres w jakim przeciwdziałają ryzyku, a poprzez to ułatwiają lub utrudniają realizację ustalonych celów i zadań.

Na podstawie dokonanej identyfikacji i oceny ryzyka oraz określenia metody przeciwdziałania ryzyku, kierujący komórkami organizacyjnymi (właściciele ryzyka) powinni wprowadzić ww. metody jego ograniczenia, a także dokonywać jego bieżącej oceny.

Ponadto zgodnie ze Standardem 2120 Międzynarodowych Standardów Praktyki Zawodowej Audytu Wewnętrznego, audyt wewnętrzny ocenia skuteczność i przyczynia się do usprawnienia procesów zarządzania ryzykiem.

Jednocześnie Audytor wewnętrzny może wykorzystywać informacje pochodzące z systemu zarządzania ryzykiem zarówno na etapie planowania rocznego, jak i przygotowywania i przeprowadzania konkretnych zadań audytowych.