WÓJT GMINY W SŁUPNIE
pow. płocki
woj. mazowieckie

ZARZĄDZENIE NR 42 / 2021
WÓJTA GMINY SŁUPNO
z dnia 8 marca 2021 r.

w sprawie wprowadzenia Regulaminu zarządzania ryzykiem w Urzędzie Gminy Słupno

Na podstawie art. 33 ust. 1 ustawy o samorządzie gminnym (Dz. U z 2020 r., poz. 713 ze zm.) w związku z art. 68 ust. 2 pkt 7 oraz art. 69 ust. 1 pkt 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2021, poz. 305) oraz art. 39 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE zarządzam, co następuje:

§ 1. Wprowadzam Regulamin zarządzania ryzykiem w Urzędzie Gminy Słupno stanowiący załącznik do zarządzenia.

§ 2. Traci moc Zarządzenie Nr 74/2012 Wójta Gminy w Słupnie z dnia 24 sierpnia 2012 r. w sprawie zarządzania ryzykiem w Urzędzie Gminy w Słupnie.

§ 3. Wykonanie zarządzenia powierza się Zastępca Wójta.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Marcin Zawadka

Załącznik
do Zarządzenia Nr 42 / 2021
Wójta Gminy Słupno
z dnia 8 marca 2021 r.

REGULAMIN ZARZĄDZANIA RYZYKIEM W URZĘDZIE GMINY SŁUPNO

§ 1

Użyte w Regulaminie określenia oznaczają:

1) **urząd** – Urząd Gminy Słupno;
2) **komórki organizacyjne** – wydziały, biura oraz samodzielne stanowiska Urzędu Gminy Słupno;
3) **kierownik komórki organizacyjnej** – naczelnika wydziału oraz samodzielne stanowisko pracy w Urzędzie Gminy Słupno;
4) **czynność przetwarzania** – powiązane ze sobą operacje na danych;
5) **analiza ryzyka** - identyfikowanie i opisywanie ryzyka oraz oszacowanie wielkości jego następstw i prawdopodobieństwa przy uwzględnieniu skuteczności istniejących zabezpieczeń, zastosowanych organizacyjnych i technicznych środków bezpieczeństwa;
6) **ryzyko** – zagrożenie związane z wystąpieniem zdarzenia lub działania, mającego negatywny wpływ na wykonywanie zadań bądź osiąganie celów oraz na zdolność Urzędu do realizacji skutecznej ochrony danych osobowych;
7) **szacowanie ryzyka** – proces oceny i analizy ryzyka;
8) **ocena ryzyka** – proces porównania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;
9) **wpływ ryzyka** – przewidywane skutki spowodowane przez zdarzenie objęte ryzykiem;
10) **prawdopodobieństwo ziszczenia się ryzyka** – możliwość występowania zdarzenia wywołującego ryzyko;
11) **poziom istotności ryzyka** – iloczyn wpływu ryzyka i prawdopodobieństwa jego wystąpienia;
12) **postępowanie z ryzykiem** – wdrażanie środków minimalizujących ryzyko do poziomu akceptowalnego;
13) **bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji oraz właściwości takie jak autentyczność, rozliczalność, niezawodność;
14) **zdarzenie związane z bezpieczeństwem informacji** – określony stan systemu, usługi lub sieci, który wskazuje na możliwość naruszenia Polityki ochrony danych osobowych lub innych procedur wewnętrznych dotyczących ochrony danych osobowych, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;
15) **incydencie związanym z bezpieczeństwem informacji** – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne zakłócenie zadań ustawowych realizowanych przez Starostwo i zagrażają bezpieczeństwu informacji;
16) **aktywa** – środki materialne i niematerialne mające wpływ na realizację celów i zadań oraz przetwarzanie danych osobowych;
17) **następstwa, skutki naruszenia praw lub wolności dla osób fizycznych** – zidentyfikowane reakcje dla określonych procesów przetwarzania danych (np.: kradzież tożsamości);
18) **organizacyjne i techniczne środki bezpieczeństwa, mechanizmy kontrolne** – polityki, zarządzenia, procedury, instrukcje, fizyczne i techniczne środki zabezpieczeń, systemy, zaprojektowane i wdrożone w celu ograniczenia prawdopodobieństwa wystąpienia i/lub następstw ryzyka. Podstawowy zestaw mechanizmów kontrolnych,

nie stanowiący katalogu zamkniętego, wszystkie działania i procedury podejmowane w celu zwiększenia prawdopodobieństwa realizacji zadań i osiągania celów to:
a) dokumentacja systemu kontroli zarządczej (procedury, instrukcje, wytyczne),
b) dokumentowanie poszczególnych zdarzeń (incydenty, naruszenia),
c) zatwierdzanie operacji, w tym finansowych,
d) podział obowiązków między pracownikami,
e) nadzór nad realizacją celów i zadań,
f) ograniczanie dostępu do zasobów materialnych, finansowych i informatycznych.

19) **proces realizowany w jednostce** – ciąg czynności zaprojektowanych, a następnie wykonywanych w ten sposób, aby w ich wyniku powstał produkt lub usługa. Procesy realizowane w Urzędzie są opisane w Rejestrze Czynności Przetwarzania;
20) **osoba zarządzająca ryzykiem** – osoba odpowiedzialna za zarządzanie danym ryzykiem;
21) **zarządzanie ryzykiem** – proces identyfikacji, oceny i przeciwdziałaniu ryzyku. Obejmuje on także monitorowanie ryzyka i środków podejmowanych w celu jego ograniczenia;
22) **akceptowalnym poziomie ryzyka** – ustalony poziom istotności ryzyka, przy którym nie jest wymagane podejmowanie działań przeciwdziałających temu ryzyku;
23) **ryzyku nieakceptowalnym** – ryzyko, które wymaga podjęcia określonych działań ograniczających je do poziomu ryzyka akceptowalnego poprzez zmniejszenie wpływu lub prawdopodobieństwa jego wystąpienia (przeciwdziałanie ryzyku).

§ 2
Podstawy funkcjonowania procesu zarządzania ryzykiem

1. Zarządzenie ryzykiem w Urzędzie Gminy Słupno obejmuje realizację celów i zadań oraz przetwarzanie danych osobowych. Jest to proces ciągły, polegający na:
1) zapewnieniu poufności, integralności, dostępności i odporności systemów oraz usług przetwarzania;
2) wdrażaniu odpowiednich środków technicznych, organizacyjnych, zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku;
3) ocenie czy wdrożony stopień bezpieczeństwa jest odpowiedni, uwzględniając ryzyko wiążące się z przetwarzaniem danych osobowych, w szczególności wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

2. Celem zarządzania ryzykiem jest:
1) usprawnienie procesu planowania;
2) zwiększenie prawdopodobieństwa realizacji zadań i osiągania zaplanowanych celów;
3) zapewnienie mechanizmów kontroli wewnętrznej;
4) zapewnienie Kierownictwu Urzędu wczesnej informacji o zagrożeniach dla realizacji wyznaczonych celów i zadań.

3. Celem procesu zarządzania ryzykiem jest także wdrożenie odpowiednich środków technicznych, organizacyjnych i informatycznych w taki sposób, aby przetwarzanie danych osobowych odbywało się zgodnie z ogólnym rozporządzeniem o ochronie danych osobowych RODO.

4. Zarządzanie ryzykiem powinno prowadzić do eliminacji lub ograniczenia – do akceptowalnego poziomu – prawdopodobieństwa i następstw wystąpienia zdarzeń negatywnych.

§ 3
Zadania kierowników komórek organizacyjnych

1. Kierownicy komórek organizacyjnych w procesie zarządzania ryzykiem odpowiadają za:
   1) identyfikację, ocenę i ograniczanie ryzyka;
   2) składanie rocznych arkuszy identyfikacji, oceny i metod przeciwdziałania ryzyku dla zadań komórki organizacyjnej oraz przetwarzania danych osobowych;
   3) określenie niezbędnych warunków umożliwiających realizację zadań związanych z osiągnięciem wyznaczonych celów;
   4) zapewnienie zgodności działań z niniejszym Regulaminem;
   5) współpracę z Zastępcą Wójta przy wykonywaniu czynności dotyczących zarządzania ryzykiem;
   6) zapewnienie, by pracownicy byli świadomi wagi procesu zarządzania ryzykiem.
2. Wzór arkusza identyfikacji, oceny i metod przeciwdziałania ryzyku dla zadań komórki organizacyjnej stanowi **załącznik nr 1** do regulaminu.
3. Wzór arkusza analizy ryzyka i zagrożeń w zakresie przetwarzania danych osobowych stanowi **załącznik nr 2** do regulaminu.

§ 4
Analiza ryzyka i zagrożeń

1. Proces analizy ryzyka ma charakter subiektywnej oceny dokonywanej przez kierowników komórek organizacyjnych.
1) **AKTYWA (ZASOBY)**, które należy chronić m.in.:
   a) sprzęt komputerowy,
   b) dane osobowe przetwarzane w formie papierowej i elektronicznej,
   c) programy i aplikacje,
   d) budynki i pomieszczenia,
   e) zasoby ludzkie,
   f) środki finansowe,
   g) mienie.
2) **ZAGROŻENIA** – czynniki, które mogą spowodować wystąpienie incydentu lub naruszenia.
3)**PODATNOŚCI** – słabość zasobów, która może być wykorzystana przez potencjalne zagrożenie.
4) **SKUTKI** – jaki wpływ będzie miał zaistniały incydent na utratę danych osobowych czy realizację zadania.
3. W ramach analizy ryzyka podejmowane są następujące działania:
   a) identyfikacja ryzyka,
   b) szacowanie ryzyka,
   c) postępowanie z ryzykiem.

§ 5
Identyfikacja ryzyka

1. Identyfikacja ryzyka polega na rozpoznaniu, określeniu i opisaniu ryzyk, które mogą wystąpić jako przeszkody w realizacji zadań/procesów realizowanych przez Urząd oraz zapewnieniu właściwego przetwarzania danych osobowych.
2. W procesie identyfikacji ryzyka uwzględnia się zagrożenia związane z wystąpieniem

jakiegokolwiek zdarzenia, działania lub braku działania, które może mieć negatywny wpływ dla osób fizycznych, których dane są przetwarzane w Urzędzie oraz dla bezpieczeństwa samej jednostki.

3. Podczas identyfikacji należy odnieść się w szczególności do:
   1) procesów realizowanych w Urzędzie – w przypadku przetwarzania danych osobowych;
   2) celów i zadań określonych w planie pracy na dany rok kalendarzowy;
   3) sposobów zabezpieczania danych osobowych.

4. Identyfikacji podlega zarówno ryzyko wewnętrzne, mające swoje źródło w działaniach podejmowanych przez pracowników Urzędu, jak i ryzyko zewnętrzne, wynikające z czynników zewnętrznych.

5. Identyfikacja ryzyka powinna uwzględniać wyniki przeprowadzonych w Urzędzie audytów oraz kontroli wewnętrznych i zewnętrznych.

6. Podczas identyfikacji ryzyka stosowane są następujące kategorie ryzyka: finansowe, zasobów ludzkich, działalności, zewnętrzne oraz związane z przetwarzaniem danych osobowych. Przykłady kategorii ryzyka określa **załącznik nr 3** do regulaminu.

§ 6
Szacowanie ryzyka

1. Szacowanie ryzyka dokonywane jest raz w roku przez kierowników komórek organizacyjnych, niezwłocznie w przypadku pojawienia się nowych zagrożeń lub po znaczących zmianach np. organizacyjnych, konieczności realizacji nowych procesów, zmianach w przepisach prawa.

2. Szacowanie ryzyka to proces polegający na:
   1) oszacowaniu szkód i strat związanych z naruszeniem bezpieczeństwa, w tym legalności poufności, integralności i rozliczalności;
   2) oszacowaniu prawdopodobieństwa wystąpienia zagrożenia i naruszenia bezpieczeństwa danych osobowych **(prawdopodobieństwa wystąpienia ryzyka**);
   3) oszacowaniu potencjalnych skutków, jakie zaistnienie danego rodzaju ryzyka (zdarzenia) może mieć dla osoby fizycznej, której dane dotyczą oraz dla Urzędu tj. **następstw (wpływu)**;
   4) określeniu **poziomu istotności ryzyka** z uwzględnieniem praw i wolności osób fizycznych, których dane dotyczą oraz bezpieczeństwa jednostki;
   5) reakcja na ryzyko tzn. określenie czy ryzyko jest akceptowalne lub nieakceptowalne i wymaga podjęcia działań.

2. Przy ocenie skutków należy wziąć pod uwagę zarówno skutki finansowe, jak i niefinansowe, np.: utratę reputacji, konsekwencje prawne, utratę szansy zrealizowania celu lub zadania, opóźnienie w realizacji, obniżenie jakości pracy.

§ 7
Postępowanie z ryzykiem

1.Dla zidentyfikowanego i poddanego analizie ryzyka, wskazana zostaje jedna z poniższych reakcji na ryzyko:
   1) Akceptowanie (tolerowanie) – oznacza, że nie podejmuje się żadnych działań zaradczych, ale rozumie się ewentualne skutki zdarzenia i świadomie godzi się na nie (np.: możliwość przeciwdziałania jest ograniczona lub koszt przeciwdziałania przewyższa potencjalne korzyści);

2) Ograniczenie – podjęcie działań zaradczych, które mają doprowadzić do likwidacji lub ograniczenia ryzyka do akceptowalnego poziomu np. poprzez wzmocnienie mechanizmów kontrolnych;
3) Dzielenie się – częściowe lub całkowite przeniesienie ryzyka na inny podmiot np.: ubezpieczyciela;
4) Unikanie ryzyka – niepodejmowanie lub zaprzestanie działania narażającego na ryzyko;

2. Decyzja odnośnie reakcji na ryzyko powinna być podejmowana z uwzględnieniem, z jednej strony potencjalnych kosztów, które wiążą się z jego ograniczaniem, z drugiej zaś potencjalnych korzyści, które wynikają z podjęcia ryzyka.

Sposób oceny prawdopodobieństwa wystąpienia ryzyka:

Prawdopodobieństwo wystąpienia ryzyka	Ilość punktów	Przesłanki
wysokie	3	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się wielokrotnie w ciągu roku.
średnie	2	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się kilka razy w ciągu roku.
niskie	1	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się raz lub nie zdarzy się w ciągu roku.

Sposób oceny skutku ryzyka:

Skutek wystąpienia ryzyka	Ilość punktów	Przesłanki
wysoki	3	Poważne zagrożenie realizacji założonych celów i zadań. Dotkliwa strata finansowa. Znaczny uszczerbek na wizerunku. Długotrwały i trudny proces przywracania stanu poprzedniego.
średni	2	Spadek efektywności działania i obniżenie jakości wykonywania zadań. Niewielka strata finansowa. Nieznaczny negatywny wpływ na wizerunek. Trudny proces przywracania stanu poprzedniego.
niski	1	Zakłócenie lub opóźnienie w wykonywaniu zadań. Bez uszczerbku dla wizerunku. Skutki łatwe do usunięcia.

Punktową istotność ryzyka (Istotność) występującego przy realizacji danego celu lub zadania określa się według wzoru: **I**stotność = **P**rawdopodobieństwo **x** **S**kutek

Mapa istotności ryzyka:

Prawdopodobieństwo				
wysokie	3	6	9	
średnie	2	4	6	
niskie	1	2	3	
	niski	średni	wysoki	Skutek

Poziomy Istotności ryzyka:

a) ryzyko **wysokie – 6 - 9** punktów;

b) ryzyko **średnie – 3 - 4** punkty;

c) ryzyko **niskie – 1 - 2** punkty.

3. Przy wskazaniu reakcji na ryzyko należy uwzględnić określony w niniejszym dokumencie akceptowalny poziom ryzyka. W tym celu należy wykorzystać mapę ryzyka. Mapa ryzyka jest graficzną prezentacją wyników oceny ryzyka. Dla każdego z poziomów ryzyka przypisano odpowiednią kolorystykę:

1) **poziom niski** – **kolor zielony** – akceptowalny poziom ryzyka, zaplanowanie i wdrożenie działań zaradczych zależy od decyzji właściciela ryzyka;
2) **poziom średni** – **kolor żółty** – nieakceptowalny poziom ryzyka, wymóg stałego monitorowania poziomu ryzyka oraz konieczność zaplanowania działań zaradczych do ewentualnego wdrożenia;
3) **poziom wysoki** – **kolor czerwony** – nieakceptowalny poziom ryzyka, konieczność wycofania się lub opracowania i wdrożenia planu działań sprowadzających ryzyko do akceptowalnego poziomu w terminie uzgodnionym z Zastępca Wójta. Właściciel ryzyka zobowiązany jest do monitorowania poziomu ryzyka i skuteczności przyjętych działań;

4. Zastosowane techniczne, organizacyjne i informatyczne środki bezpieczeństwa, mechanizmy kontrolne to działania zaradcze, które mają na celu ograniczenie ryzyka do poziomu akceptowalnego – zarówno prawdopodobieństwa, jak i następstw jego wystąpienia.
5. Mechanizmy kontrolne powinny prowadzić do zmniejszenia niepewności wyników poprzez wykrycie i skorygowanie niepożądanych rezultatów, unikanie niepożądanych efektów lub ograniczenie ich występowania, a także osiągnięcie spodziewanych rezultatów.
6. W odniesieniu do każdego rodzaju ryzyka ustalana jest osoba odpowiedzialna za zarządzanie danym ryzykiem – właściciel ryzyka.
7. Do zadań właściciela ryzyka należy, w szczególności:

1) identyfikacja i ocena ryzyk związanych z realizacją przypisanych procesów;
2) określenie istniejących zabezpieczeń, zastosowanych środków technicznych, organizacyjnych i informatycznych;
3) określenie następstw naruszeń praw lub wolności dla osób fizycznych;

4) określenie prawdopodobieństwa, następstw wystąpienia i istotności ryzyka w kontekście następstw dla osób fizycznych;
5) określenie reakcji w odniesieniu do poszczególnych ryzyk;
6) określenie następstw dla Urzędu oraz w przypadku danych osobowych – określenie skutków dla osoby fizycznej, której dane dotyczą;
7) realizacja organizacyjnych, technicznych i informatycznych środków bezpieczeństwa w stosunku do zidentyfikowanych ryzyk.

§ 8
Reakcja na ryzyko

1. Kierownicy komórek organizacyjnych przekazują wypełnione i podpisane arkusze ryzyk do Zastępcy Wójta w terminie do 31 grudnia na rok następny. Analiza ryzyka na rok 2021 zostanie opracowana do 31 marca 2021 r.
2. Na podstawie złożonych arkuszy, Zastępca Wójta sporządza rejestr ryzyk nieakceptowalnych na dany rok i przedkłada go do zatwierdzenia Wójtowi.
3. Rejestr ryzyk wykorzystywany jest do poprawy efektywności zarządzania ryzykiem oraz usprawnienia systemu kontroli zarządczej.

§ 9

Analiza ryzyka i zagrożeń w obszarze przetwarzania danych osobowych

WYTYCZNE DOTYCZACE OSZCOWANIA SZKÓD I STRAT ZWIĄZANYCH Z NARUSZENIEM BEZPIECZEŃSTWA

Lp.	Przesłanki przetwarzania danych osobowych	Definicja	Możliwe zagrożenia dla bezpieczeństwa danych osobowych
1.	**Legalność** (Zgodność z prawem, rzetelność, przejrzystość)	Zapewnienie przetwarzania danych osobowych w sposób zgodny z prawem, rzetelny i przejrzysty dla osoby, której dane dotyczą.	Zagrożeniem może być przetwarzanie danych osobowych niezgodnie z prawem. Przetwarzanie w celach innych, dla których dane zostały zebrane. Zbieranie danych osobowych „na zapas" dla przyszłych nieoznaczonych jeszcze celów. Brak uaktualniania danych.
2.	**Poufność**	Zapewnienie, że dane osobowe nie będą udostępniane nieupoważnionym osobom.	Zagrożenia w zakresie poufności mogą obejmować: – nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są dane osobowe; – ujawnienie haseł dostępu do stanowiska komputerowego; – nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik; – utrata nośnika zawierającego dane osobowe; – klęska żywiołowa, w wyniku, której utracono poufność danych osobowych; – nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym; – podsłuch i podgląd danych osobowych; – niekontrolowane wynoszenie danych osobowych poza obszar przetwarzania; – pokonanie zabezpieczeń fizycznych bądź programowych;

			– naprawy i konserwacja systemów lub sieci teleinformatycznej służących do przetwarzania danych osobowych przez osoby nieuprawnione do przetwarzania danych osobowych, – brak nadzoru nad osobami sprzątającymi, – brak nadzoru nad dokumentami zawierającymi dane osobowe, – brak nadzoru nad funkcjonowaniem monitoringu wizyjnego, – brak polityki zarządzania kluczami, – niestosowanie polityki „czystego biurka" i „czystego ekranu", – praca zdalna
3.	**Integralność**	Zapewnienie, że dane osobowe będą chronione przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem za pomocą odpowiednich środków technicznych lub organizacyjnych.	Zagrożenia w zakresie integralności mogą obejmować: – nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego; – błędy, pomyłki – brak mechanizmów uniemożliwiających skasowanie lub zmianę loginów przez administratora lub innego użytkownika; – wadliwe działanie systemu operacyjnego – wirus – brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność; – zagrożenia zewnętrzne, – brak sporządzania kopii zapasowych, – użytkowanie nielegalnego oprogramowania, – niezabezpieczony serwer, – brak możliwości podtrzymania zasilania w przypadku spadku lub braku prądu, – praca zdalna
4.	**Rozliczalność**	Możliwość wykazania, że przestrzegane są przepisy prawa w zakresie ochrony danych osobowych. Działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.	Zagrożenia w zakresie rozliczalności mogą obejmować: – brak kontroli nad dokumentami wykonywanymi na stanowisku pracy w zakresie kopiowania i drukowania; – brak możliwości identyfikacji użytkownika na stanowisku komputerowym, gdzie przetwarza się dane osobowe, indywidualne identyfikatory, rejestr użytkowników; – nieuprawnione wprowadzenie zmian w treści dokumentu zawierającego dane osobowe; – błędy oprogramowania lub sprzętu, niewłaściwa konfiguracja systemu informatycznego; – błędy w administrowaniu systemem informatycznym; – niespełnianie przez system informatyczny wymagań z zakresu bezpieczeństwa danych osobowych; – brak rejestracji udostępniania danych, – brak odpowiednich procedur, – brak regularnych audytów i kontroli w obszarze przetwarzania danych osobowych, – brak wyznaczenia inspektora ochrony danych, – brak upoważnienia pracowników do przetwarzania danych osobowych,

			– brak oświadczeń pracowników o zachowaniu poufności, – brak rejestru czynności przetwarzania danych osobowych, – brak procedury postępowania w przypadku wystąpienia incydentu w obszarze przetwarzania danych osobowych.

Załącznik
do Zarządzenia Nr 42 / 2021
Wójta Gminy Słupno
z dnia 8 marca 2021 r.

WYTYCZNE DO OCENY PRAWDOPODOBIEŃSTWA WYSTĄPIENIA I NASTĘPSTW RYZYKA

Prawdopodobieństwo wystąpienia (lub/i)	Oszacowane ryzyko
Tego typu ryzyko wystąpiło 1 raz w okresie ostatnich 3 lat. Ryzyko prawdopodobnie nie wystąpi/może wystąpić w zupełnie wyjątkowych sytuacjach,. Przy realizacji danego zadania/procesu współpracuje się z małą (1 lub 2) liczbą komórek/jednostek. W okresie ostatnich 3 lat obszar/proces podlegał zmianom organizacyjnym i kadrowym w minimalnym stopniu i uznaje się je za wdrożone. Zadania/proces w małym zakresie objęty regulacjami o charakterze zewnętrznym. Nie podlegały one zmianom.	**1** **niskie**
Tego typu ryzyko wystąpiło 2 razy w okresie ostatnich 3 lat. Przy realizacji danego celu współpracuje się z dużą (co najmniej 3) liczbą komórek/jednostek. Zadanie/proces podlegał zmianom organizacyjnym, i kadrowym które zakończyły się ponad rok temu, Zadanie/proces objęty w małym stopniu regulacjami zewnętrznymi, które mogły podlegać w ostatnim okresie pewnym zmianom. Tego typu ryzyko wystąpiło 3 razy w okresie ostatnich 3 lat. Istnieje wysokie prawdopodobieństwo na wystąpienie tego ryzyka, Zadanie/proces wymaga współpracy z dużą (więcej niż 3) liczbą komórek i jednostek lub/i podmiotami zewnętrznymi. W ciągu ostatniego roku obszar/proces podlegał zmianom organizacyjnym i kadrowym, z których część może wymagać	**2** **średnie**

Następstwa (wpływ)	Oszacowane ryzyko
Dla osoby fizycznej, której dane dotyczą: – utrata kontroli nad własnymi danymi – naruszenie dobrego imienia – konieczność ponownego dostarczenia dokumentów **Dla jednostki:** – naruszenie poufności danych – kara finansowa – niemożność świadczenia usług – konsekwencje prawne (skarga do UODO, postępowanie administracyjne i sądowe) – przerwa w działaniu Urzędu – niezdolność do wypełnienia zobowiązań finansowych wobec interesantów bądź kontrahentów – niezdolność do wypełnienia zobowiązań wynikających z zawartych umów/porozumień	**1** **małe**
Dla osoby fizycznej, której dane dotyczą: – utrata kontroli nad własnymi danymi – naruszenie dobrego imienia – konieczność ponownego dostarczenia dokumentów – dyskryminacja – szkoda materialna **Dla jednostki:** – naruszenie poufności danych – kara finansowa – niemożność świadczenia usług – konsekwencje prawne (skarga do UODO, postępowanie administracyjne i sądowe) – przerwa w działaniu Urzędu – niezdolność do wypełnienia zobowiązań finansowych wobec interesantów bądź kontrahentów – niezdolność do wypełnienia zobowiązań wynikających z zawartych umów/porozumień	**2** **średnie**

Prawdopodobieństwo wystąpienia (lub/i)	Oszacowane ryzyko	Następstwa (wpływ)	Oszacowane ryzyko
poprawek i działań dostosowawczych. Obszar/proces objęty dużą liczbą regulacji prawnych (zewnętrznych i wewnętrznych), które w ostatnim roku podlegały istotnym zmianom.		– utrata dostawców i kontrahentów – zwolnienie pracownika	
Tego typu ryzyko wystąpiło więcej niż 3 razy w okresie ostatnich 3 lat. Istnieje bardzo wysokie prawdopodobieństwo na wystąpienie tego ryzyka. Zadanie/proces wymaga współpracy z bardzo dużą (więcej niż 10) liczbą jednostek lub/i podmiotami zewnętrznymi. W ostatnim roku zadanie/proces podlegał istotnym zmianom organizacyjnym i kadrowym albo obszar podlega częstym zmianom tego typu bądź też obszar jest w trakcie zmian. Obszar/proces objęty dużą liczbą regulacji prawnych (zewnętrznych i wewnętrznych), które w ostatnim roku podlegały istotnym zmianom lub/i, które zmienią się z pewnością w ciągu najbliższego roku.	**3 wysokie**	**Dla osoby fizycznej, której dane dotyczą:** – utrata kontroli nad własnymi danymi – naruszenie dobrego imienia – konieczność ponownego dostarczenia dokumentów – dyskryminacja – szkoda materialna **Dla jednostki:** – naruszenie poufności danych – kara finansowa – niemożność świadczenia usług – konsekwencje prawne (skarga do UODO, postępowanie administracyjne i sądowe) – przerwa w działaniu Urzędu – niezdolność do wypełnienia zobowiązań finansowych wobec interesantów bądź kontrahentów – niezdolność do wypełnienia zobowiązań wynikających z zawartych umów/porozumień – utrata dostawców i kontrahentów – zwolnienie pracownika – szkoda społeczna – strata finansowa	**3 wysokie**

pieczęć
komórki organizacyjnej

Arkusz identyfikacji, oceny oraz metod przeciwdziałania ryzyku
dla celów .....na rok.....
(nazwa komórki organizacyjnej Starostwa)

Identyfikacja i ocena ryzyka								**Przeciwdziałanie ryzyku**	
L.p.	Cel	Ryzyko (wraz z podaniem kategorii)	Wpływ	Prawdopodobieństwo	Poziom istotność ryzyka	Ewaluacja ryzyka	Postępowanie z ryzykiem (A,O,D,U)	Planowana metoda przeciwdziałania ryzyku	Osoba zarządzająca ryzykiem
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*

.....
podpis Kierownika komórki organizacyjnej

Data sporządzenia .....

.....
(data i podpis Zastępcy Wójta)

Załącznik nr 2
do Regulaminu zarządzania ryzykiem w Urzędzie Gminy Słupno

Arkusz analizy ryzyka i zagrożeń w zakresie przetwarzania danych osobowych w.....
(nazwa komórki organizacyjnej)

Lp.	Opis procesu przetwarzania danych osobowych	Aktywa/zasoby które należy chronić	Identyfikacja ryzyka/zagrożenia	Istniejące zabezpieczenia / Zastosowane oraganizacyjne i techniczne środki bezpieczeństwa /mechanizmy kontrolne	Następstwa/skutki naruszenia praw lub wolności dla osób fizycznych	Prawa i wolności osób fizycznych kryteriów			Identyfikacja zagrożeń bezpieczeństwa informacji	JEDNOSTKA			Ocena ryzyka po uwzględnieniu kryteriów (9+13)/2	RYZYKO (N, Ś, W, K)	Następstwa/ skutki dla jednostki	Reakcja na ryzyko (O, D, A, U)	Działania zaradcze	Osoba zarządzająca ryzykiem	Ewaluacja ryzyka dla całego procesu
						P - prawdopodobieństwo w skali od 1 od 5	W - wpływ w skali od 1 do 5	Istotność (7x8)		P - prawdopodobieństwo w skali od 1 od 5	W - wpływ w skali od 1 do 5	Istotność (11x12)							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1.																			

Kategorie ryzyka

Poniższa tabela przedstawia kategorie ryzyka wraz z **przykładami** dotyczącymi jego możliwych źródeł oraz skutków.

Tabela nie określa zamkniętego katalogu ryzyka.

Kategoria ryzyka	
Ryzyko finansowe	
Budżetowe	Związane z planowaniem dochodów i wydatków, dostępnością środków publicznych, dokonywaniem wydatków i pobieraniem dochodów.
Oszustwa i kradzieży	Związane ze stratą środków rzeczowych i finansowych będących wynikiem przestępstwa lub wykroczenia.
Podlegające ubezpieczeniu	Związane ze stratami finansowymi, które mogą być przedmiotem ubezpieczenia np. ryzyko pożaru, wypadku.
Zamówień publicznych i zlecania zadań publicznych	Związane z podejmowaniem decyzji oraz udzielaniem zamówień publicznych lub zlecaniem zadań publicznych innym podmiotom np. ryzyko naruszenia zasad lub trybu określonego w zamówieniach publicznych.
Odpowiedzialności	Związane z obowiązkiem zapłaty kwot pieniężnych tytułem np. odszkodowań, odsetek karnych, kosztów procesowych.
Realizacja programów współfinansowanych ze środków UE.	Związane z wystąpieniem nieprawidłowości przy wykorzystaniu środków z UE.
Ryzyko dot. zasobów ludzkich	
Zarządzanie zasobami ludzkimi	Związane z liczebnością i kompetencjami pracowników, szkoleniami, wprowadzaniem nowych zadań bez zabezpieczenia etatowego.
Bhp	Związane ze zdrowiem pracowników i wypadkami przy pracy.
Ryzyko działalności	
Organizacji i podejmowania decyzji	Związane ze strukturą organizacyjną, organizacją pracy oraz przekazywaniem obowiązków i uprawnień np. ryzyko nieprecyzyjnie określonych obowiązków, ryzyko braku formalnie powierzonych obowiązków, ryzyko nieodpowiedniej struktury organizacyjnej, ryzyko nieprawidłowo wydanej decyzji.
Kontroli wewnętrznej	Związane z funkcjonowaniem systemu kontroli wewnętrznej np. ryzyko niedostatecznej kontroli, ryzyko nieskutecznych mechanizmów kontrolnych.
Informacji	Związane z jakością informacji, na podstawie których podejmowane są decyzje np. ryzyko niesprawdzonej lub niepełnej informacji.
Reputacji	Związane z reputacją Urzedu np. ryzyko negatywnych opinii.
Systemów informatycznych	Związane z używanymi w Urzędzie systemami i programami informatycznymi oraz ochroną zawartych w nich danych np. ryzyko awarii, ryzyko udostępnienia danych osobom nieuprawnionym, ryzyko nieuprawnionej modyfikacji danych.

Regulacji wewnętrznych	Związane z istnieniem i adekwatnością regulacji wewnętrznych.
Ryzyko zewnętrzne	
Infrastruktury	Związane z infrastrukturą, np. wyposażeniem, bazą lokalową, środkami transportu i środkami łączności.
Gospodarcze	Związane z czynnikami ekonomicznymi, np. inflacja.
Środowiska prawnego	Związane ze skomplikowaniem i zmianami prawa oraz niejednolitym orzecznictwem.