# ZASADY I TRYB ZARZĄDZANIA RYZYKIEM OCHRONY DANYCH OSOBOWYCH PRZETWARZANYCH W OŚRODKU POMOCY SPOŁECZNEJ W STARYM SĄCZU

**§ 1**. Ilekroć w Zasadach jest mowa o:

1) **Administratorze Danych Osobowych ( ADO )** – należy przez to rozumieć Ośrodek Pomocy Społecznej w Starym Sączu zwany dalej "Ośrodkiem" reprezentowany przez Kierownika Ośrodka;

2) **RODO** – należy przez to rozumieć rozporządzenie Parlamentu Europejskiego i Rady (UE) 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L Nr 119 s. 1)

3) **Inspektorze Ochrony Danych (IOD)** – należy rozumieć osobę wyznaczoną na podstawie art. 37 ust. 1 lit. a RODO przez Burmistrza Starego Sącza;

4) **Zasadach** – należy przez to rozumieć Zasady i tryb zarządzania ryzykiem bezpieczeństwa danych osobowych w Ośrodku;

5) **ryzyku** – należy przez to rozumieć możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów; ryzyko jest mierzone wpływem (skutkami) oraz prawdopodobieństwem wystąpienia;

6) **aktywach** – należy przez to rozumieć wszystko to, co ma wartość dla Ośrodka oraz jego Kierownika, jako administratora danych osobowych przetwarzanych w tej jednostce. Do aktywów (podstawowych i wspierających) Ośrodka zaliczyć można procesy przetwarzania danych osobowych, wszelkie informacje dotyczące funkcjonowania Ośrodka, w tym przetwarzane dane osobowe, pracowników, siedzibę, organizację, sprzęt, oprogramowanie informatyczne, czy sieć komputerową;

7) **istotności ryzyka** – należy przez to rozumieć iloczyn prawdopodobieństwa wystąpienia ryzyka oraz potencjalnego wpływu jego wystąpienia;

8) **kontekście** – należy przez to rozumieć wszystkie informacje wiążące się z działaniem Ośrodka, w tym informacje dotyczące środowiska prawnego, społecznego, finansowego czy też technologicznego, np. przepisy prawne, obowiązujące procedury wewnętrzne;

9) **podatności** – należy przez to rozumieć słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki dla Ośrodka, jak np. luka w systemie informatycznym;

**§ 2 . 1**. Celem opracowanych Zasad jest ustalenie metodyki zarządzania ryzykiem bezpieczeństwa danych osobowych przetwarzanych w Ośrodku z uwzględnieniem ryzyka naruszenia praw lub wolności osób fizycznych, których dane dotyczą.

**2**. Zasady określają sposób przeprowadzania i dokumentowania procesu szacowania ryzyka ochrony danych osobowych.

**§ 3. 1**. Wynikiem przeprowadzonego procesu szacowania ryzyka jest określenie adekwatnych do zagrożeń i prawdopodobieństwa ich wystąpienia, mechanizmów technicznych i organizacyjnych służących przeciwdziałaniu ryzyka.

**2**. Zarządzanie ryzykiem ma na celu prowadzenie działań podnoszących poziom bezpieczeństwa ochrony danych osobowych przetwarzanych w jednostce uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych. Oznacza to między innymi, że dane osobowe przetwarzane w jednostce powinny być zabezpieczone przed nieuprawnionymi

zmianami, ujawnieniem nieupoważnionym osobom, zniszczeniem, utratą lub uszkodzeniem. Czynności podejmowane w ramach tych działań oraz zastosowane środki techniczne i organizacyjne będą zależne od środowiska, w jakim dane są przetwarzane.

**3.** Pojęcie ochrony danych należy utożsamiać z pojęciem bezpieczeństwa informacji, przez które należy rozumieć zachowanie **poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności**. Wymienione właściwości, wg definicji zawartych w PN-I13335-13 polegają odpowiednio na:

**1) poufność** – zapewnieniu, że informacja nie jest udostępniania lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom;

**2) integralność** – zapewnieniu, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

**3) dostępność** – zapewnieniu bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot;

**4) rozliczalność** – zapewnieniu, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

**5) autentyczność** – zapewnieniu, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji);

**6) niezaprzeczalność** – braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;

**7) niezawodność** – zapewnieniu spójności oraz zamierzonych zachowań i skutków.

**4**. Poprzez zarządzanie ryzykiem bezpieczeństwa ochrony danych osobowych należy rozumieć działania polegające na:

1) identyfikacji procesów;

2) określeniu zagrożeń;

3) szacowaniu ryzyka;

4) postępowaniu z ryzykiem;

5) akceptowaniu ryzyka;

6) monitorowaniu ryzyka;

7) informowaniu o ryzyku w odniesieniu do zidentyfikowanego procesu przetwarzania danych osobowych.

**§ 4.** Monitorowanie procesu zarządzania ryzykiem bezpieczeństwa danych osobowych w jednostce i dokumentowanie tych czynności jest elementem wywiązania się z ciążącego na Administratorze Danych Osobowych – Kierowniku Ośrodka – obowiązku zapewnienia przetwarzana zgodnego z RODO.

**§ 5. 1**. ADO - Kierownik Ośrodka zapewnia warunki niezbędne do prawidłowego funkcjonowania procesu zarządzania ryzykiem bezpieczeństwa danych osobowych w Ośrodku.

**2.** Proces szacowania ryzyka ochrony danych osobowych przetwarzanych w Ośrodku nadzoruje IOD.

**3.** ADO – Kierownik Ośrodka zapewnia i odpowiada za systematyczną identyfikację procesów i zagrożeń, przeprowadzanie szacowania ryzyka, ocenę jego istotności i postępowania z ryzykiem bezpieczeństwa danych osobowych w celu zapewnienia zgodnego z RODO oraz dokumentowania całego procesu zarządzania ryzykiem, spełniając tym samym wymóg rozliczalności podejmowanych działań.

**§ 6. 1.** Na analizę ryzyka składa się: szacowanie ryzyka, postępowanie z ryzykiem oraz akceptowanie ryzyka.

**2**. Szacowanie ryzyka ma na celu określenie co może się zdarzyć (kiedy, gdzie, jak i dlaczego) oraz jak dotkliwe straty mogą powstać i polega na:

1) identyfikowaniu zagrożeń;

2) analizie ryzyka;

3) ocenie ryzyka.

**3.** W ramach identyfikacji zagrożeń określany jest:

1) kontekst;

2) identyfikacja aktywów;

3) identyfikacja zagrożeń dla aktywów;

4) identyfikacja istniejących zabezpieczeń;

5) identyfikacja podatności;

6) identyfikacja następstw – skutków.

**4**. Posiadając zidentyfikowane aktywa, zagrożenia oraz zastosowane zabezpieczenia można przeprowadzić identyfikację podatności na urzeczywistnienie się określonych zagrożeń. Istotne jest, że samo istnienie podatności nie powoduje jeszcze szkody. Jej powstanie jest możliwe dopiero po zmaterializowaniu się zagrożenia, które wykorzysta daną podatność. Analiza podatności dotyczy aktywów podstawowych – przetwarzanych danych i zastosowanych do przetwarzania urządzeń – jak i wspierających – sprzęt, oprogramowanie, sieć komputerowa, pracownicy, siedziba, organizacja.

**5**. W przypadku aktywów, jakim jest np. rejestr czynności przetwarzania danych osobowych, podatnością może być sam fakt wykorzystania danych w innym celu niż zamierzony.

**6**. Dokonanie analizy ryzyka polega na:

1) oszacowaniu następstw ze szczególnym uwzględnieniem możliwości naruszenia praw lub wolności osób fizycznych;

2) oszacowaniu prawdopodobieństwa incydentu;

3) określeniu poziomu ryzyka.

**7.** Oceniając następstwa urzeczywistnienia się zagrożeń, w przypadku danych osobowych, należy uwzględnić, poza innymi czynnikami, także dotkliwe, przewidziane w RODO kary finansowe, które mogą być nakładane przez organ nadzorczy na Administratora i podmioty przetwarzające w przypadku niewywiązywania się przez nie z nałożonych obowiązków właściwej ochrony danych. Szacowanie następstw dla określonych zagrożeń powinno uwzględniać zarówno materialny, jak i niematerialny charakter.

**8.** Przyjmuje się, że zasadniczym rodzajem reakcji na ryzyko jest działanie lub przeniesienie ryzyka. Przeniesienie oznacza przekazanie ryzyka podmiotowi zewnętrznemu, np. ubezpieczenie budynku będącego siedzibą Ośrodka, powierzenie przetwarzania danych osobowych w drodze umowy przy zastosowaniu zasad zgodnych z RODO, ze wskazanymi obowiązującymi normami. Działanie może obejmować w szczególności ustanowienie nowych lub zintensyfikowanie istniejących mechanizmów kontroli, a także działania o innym charakterze (np. przeszkolenie pracowników, wprowadzenie zmian organizacyjnych, wystąpienie o dodatkowe środki finansowe, wprowadzenie dodatkowych wymogów informacyjnych, podjęcie lub nasilenie działań kontrolnych itp.).

**§ 7. 1.** Proces szacowania ryzyka w sposób określony powyżej, kończy jego ocena i ustalenie planu postępowania w przypadku wystąpienia ryzyka wysokiego i poważnego.

**2. Identyfikacja ryzyka jest dokonywana w odniesieniu do procesów określonych w Rejestrze czynności przetwarzania danych osobowych w (RCPDO).**

**3.** Coroczne szacowanie ryzyka należy przeprowadzić dla określonych procesów. W zależności od zmiany realizowanych zadań, celu, sposobu przetwarzania oraz rodzaju danych procesy te mogą ulegać zmianie lub obejmować inny zakres danych osobowych, czy działań w odniesieniu do tych samych danych osobowych. Dlatego dopuszcza się ewoluowanie procesów.

**§ 8. 1.** Identyfikację zagrożeń ochrony danych osobowych przetwarzanych w Ośrodku w ramach zidentyfikowanych procesów przeprowadza Kierownik Ośrodka lub wskazany pracownik odpowiedzialny za realizację danego procesu.

**2.** Wyniki identyfikacji, o której mowa w ust. 1, pracownik przekazuje Kierownikowi.

**§ 9. 1.** Kierownik Ośrodka wraz z pracownikami odpowiedzialnymi za dany proces przeprowadzają w ramach danego procesu analizę ryzyka, na którą składa się: szacowanie ryzyka, postępowanie z ryzykiem, akceptowanie ryzyka.

**2**. Określenie prawdopodobieństwa wystąpienia ryzyka polega na ocenie możliwości wystąpienia danego zdarzenia. Do określenia prawdopodobieństwa stosowana jest następująca skala ocen: **1** – niskie, **2** – średnie, **3** – wysokie, **4**– bardzo wysokie.

**3**. Określenie wpływu ryzyka polega na ocenie przewidywanego stopnia konsekwencji zagrożeń dla bezpieczeństwa danych osobowych w tym skutków dla osób fizycznych i podjęcia działań w celu ich zminimalizowania. Do określenia sposobu oceny skutku wystąpienia ryzyka używana jest następująca skala ocen: **1** – niski, **2** – średni, **3** – wysoki, **4** – bardzo wysoki,

**4.** Przykładowe skutki wystąpienia zidentyfikowanego ryzyka zostały określone w załączniku **Nr 1** do Zasad. Skutki dla osób fizycznych, których prawa lub wolności zostały naruszone określa motyw 85 RODO:

1) utrata kontroli nad własnymi danymi osobowymi;
2) ograniczenie praw;
3) dyskryminacja;
4) kradzież lub sfałszowanie tożsamości;
5) strata finansowa;
6) nieuprawnione odwrócenie pseudonimizacji
7) naruszenie dobrego imienia;
8) naruszenie poufności danych osobowych chronionych tajemnicą zawodową;
9) wszelkie inne znaczne szkody gospodarcze lub społeczne.

**5.** Zasady oceny wpływu ryzyka oraz prawdopodobieństwa jego wystąpienia określa załącznik **Nr 2** do Zasad.

**6.** Na podstawie dokonanej oceny prawdopodobieństwa wystąpienia ryzyka oraz wpływu jego wystąpienia określa się poziom istotności danego ryzyka. Ustala się następujące możliwe poziomy istotności ryzyka:

1) ryzyko poważne, tj. ryzyko, dla którego iloczyn prawdopodobieństwa wystąpienia danego zdarzenia oraz jego wpływu wynosi 12 -16 punktów;
2) ryzyko wysokie, tj. ryzyko, dla którego iloczyn prawdopodobieństwa wystąpienia danego zdarzenia oraz jego wpływu wynosi 9 - 11 punktów;
3) ryzyko umiarkowane, tj. ryzyko, dla którego iloczyn prawdopodobieństwa wystąpienia danego zdarzenia oraz jego wpływu wynosi 5 - 8 punktów;
4) ryzyka nieznaczne, tj. ryzyko, dla którego iloczyn prawdopodobieństwa wystąpienia danego zdarzenia oraz jego wpływu wynosi 1 - 4 punktów.

**7.** Ryzykiem akceptowalnym jest ryzyko nieznaczne i umiarkowane. Ryzyko wysokie i ryzyko poważne jest ryzykiem przekraczającym akceptowalny poziom i wymaga określenia rodzaju reakcji na ryzyko – przeciwdziałania ryzyku.

**8**. W celu określenia rodzaju reakcji na ryzyko należy przeanalizować:

1) przyczyny ryzyka i możliwe scenariusze rozwoju wydarzeń;
2) skuteczność funkcjonujących mechanizmów kontroli.

**9.** Reakcja na ryzyko może obejmować:

1) działanie – reakcje mające na celu wyeliminowanie danego ryzyka lub uwarunkowań z nim związanych w celu ochrony przed skutkami osób fizycznych;

2) łagodzenie – zmniejszanie prawdopodobieństwa lub skutków niekorzystnego zdarzenia do akceptowalnego poziomu;

3) przeniesienie – próba transferu skutków wystąpienia ryzyka na inny podmiot;

4) akceptację – aktywną (stworzenie planu działań na wypadek wystąpienia ryzyka wysokiego i poważnego) lub bierną (niepodejmowanie żadnych działań do momentu wystąpienia ryzyka – dopuszczalna tylko wtedy, gdy nie ma możliwości ograniczenia ryzyka przez działanie, bądź koszty podjętych działań przekraczają możliwe do uzyskania korzyści).

**10**. W razie potrzeby można stosować kombinację rodzajów reakcji na ryzyko.

**§ 10. 1.** Na podstawie dokonanej identyfikacji i analizy ryzyka oraz po ustaleniu rodzaju reakcji na ryzyko, wypełniany jest Arkusz szacowania ryzyka ochrony danych osobowych. Wzór i zasady wypełniania Arkusza określa załącznik **Nr 3** do Zasad.

**2**. Arkusz szacowania ryzyka ochrony danych osobowych wypełnia się i 1 egz. przekazuje Inspektorowi Ochrony Danych **do dnia 30 września każdego roku**. Na podstawie oszacowanego ryzyka sporządza się zbiorczy raport.

**§ 11.1.** Na podstawie zbiorczego raportu szacowania ryzyka ochrony danych osobowych przetwarzanych w Ośrodku, podejmowane są planowane działania w celu zmniejszenia ryzyka do akceptowalnego poziomu.

**2.** W przypadku zidentyfikowania nowego ryzyka przekraczającego akceptowalny poziom ryzyka, ADO – Kierownik Ośrodka określa rodzaj reakcji na ryzyko oraz planowane działania w celu jego zmniejszenia do akceptowalnego poziomu.

**§ 12**. ADO – Kierownik Ośrodka na bieżąco monitoruje i ocenia skuteczność działań podejmowanych w celu zmniejszenia ryzyka przetwarzania danych osobowych do akceptowalnego poziomu.

.....

( podpis Administratora Danych – Kierownika Jednostki )

## Przykładowe skutki zaistnienia ryzyka

Dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności.

**Skutek prawny:**
1) wystąpienie zagrożenia nie doprowadzi do naruszenia przepisów prawa;
2) wystąpienie zagrożenia doprowadzi do naruszenia przepisów prawa, z wyłączeniem przepisów karnych, lub w przypadku niepodjęcia odpowiednich działań naprawczych naruszenie prawa zostanie nieuniknione;
3) bezpośrednią konsekwencją wystąpienia zagrożenia jest naruszenie przepisów karnych.

**Skutek finansowy:**
1) wystąpienie zagrożenia nie spowoduje strat finansowych;
2) wystąpienie zagrożenia spowoduje straty finansowe w maksymalnej wysokości do 100 tys. zł;
3) wystąpienie zagrożenia spowoduje straty finansowe w wysokości powyżej 100 tys. zł.

**Skutek wizerunkowy:**
1) wystąpienie zagrożenia nie ma wpływu na wizerunek jednostki lub ten wpływ jest znikomy, nie wiąże się z zaangażowaniem środków organizacyjno-finansowych w celu odbudowania wizerunku;
2) wystąpienie zagrożenia ma mało znaczący negatywny wpływ na wizerunek jednostki lub krótkoterminową utratę wizerunku, wiąże się z zaangażowaniem środków organizacyjno-finansowych w celu odbudowania wizerunku w maksymalnej wysokości do 100 tys. zł;
3) wystąpienie zagrożenia powoduje istotny lub duży negatywny wpływ na wizerunek jednostki, wiąże się z zaangażowaniem środków organizacyjno-finansowych w celu odbudowania wizerunku w wysokości powyżej 100 tys. zł

……..
(podpis Administratora Danych – Kierownika Jednostki)

## Prawdopodobieństwo wystąpienia ryzyka

Prawdopodobieństwo ( P ) wystąpienia ryzyka wiąże się z niepewnością wystąpienia ewentualnego zdarzenia. Szacowanie prawdopodobieństwa jest kwestią subiektywnej oceny. Przy szacowaniu prawdopodobieństwa wystąpienia ryzyka uwzględnia się:
- częstotliwość wystąpienia zdarzenia,
- rodzaj ryzyka,
- czynniki środowiskowe,
- rodzaje podatności,
- istniejące mechanizmy przeciwdziałania ryzyka ( zabezpieczenia )

Sposób oceny prawdopodobieństwa wystąpienia ryzyka powinno nastąpić na podstawie jakościowo – ilościowej oceny, wg poniższej tabeli.

| **Prawdopodobieństwo wystąpienia ryzyka** | **Ilość punktów** | **Przesłanki** |
|---|---|---|
| Bardzo wysokie (81-100%) | **4** | Przewiduje się, że zdarzenie z pewnością wystąpi w ciągu roku |
| Wysokie (61-80%) | **3** | Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się wielokrotnie w ciągu roku |
| Średnie (21-60%) | **2** | Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się raz lub kilka razy w ciągu roku |
| Niskie (0-20%) | **1** | Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się raz lub nie zdarzy się w ciągu roku |

## Wpływ (skutek ) wystąpienia ryzyka

Wpływ (W) (skutek ) wystąpienia ryzyka związany jest z określeniem sytuacji po wystąpieniu ryzyka związanego z naruszeniem praw i wolności osób fizycznych. Określenie potencjalnych skutków wystąpienia danego ryzyka dokonuje się w oparciu o jakościowo – ilościową ocenę wg. poniższej tabeli.

| **Wpływ (skutek) wystąpienia ryzyka** | **Ilość punktów** | **Przesłanki – opis szczegółowy** |
|---|---|---|
| Bardzo wysoki | **4** | Poważna niezgodność z przepisami prawa. Brak procedur dla danego procesu. Olbrzymie zakłócenia pracy. Znaczny uszczerbek na wizerunku. Zagrożenia spowodują brak zachowania ciągłości procesów działania, |

| | | |
|---|---|---|
| | | utrzymania funkcjonalności systemów niezbędnych do wykonywania podstawowych celów. Brak osiągnięcia kluczowych celów. Straty finansowe. |
| Wysoki | **3** | Duże zagrożenie realizacji kluczowych zadań albo osiągania założonych celów. 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 |

**Ocena istotności ryzyka**

Określenie prawdopodobieństwa ( P ) i wpływu ryzyka w czterostopniowej skali umożliwia ustalenie współczynnika istotności ryzyka ( IR ) jako iloczynu ( wyrażonych punktowo ) prawdopodobieństwa wystąpienia ryzyka ( P ) oraz potencjalnego wpływu jego wystąpienia ( W ):

**IR = P x W**

Z uwagi na czterostopniową skalę zarówno prawdopodobieństwa ( P ) jak i wpływu wystąpienia ryzyka ( W ) współczynnik istotności ryzyka może mieć wartość od 1 do 16. Po przeprowadzonej analizie wartości przyporządkowane tym czynnikom należy przenieść na mapę punktowej oceny ryzyka, którą przedstawiono poniżej:

**Punktowa mapa ryzyka**

| **Wpływ** | | | | | |
|---|---|---|---|---|---|
| Bardzo wysoki 4 | 4 | 8 | 12 | 16 | |
| Wysoki 3 | 3 | 6 | 9 | 12 | |
| Średni 2 | 2 | 4 | 6 | 8 | |
| Niski 1 | 1 | 2 | 3 | 4 | |
| | Niskie 1 | Średnie 2 | Wysokie 3 | Bardzo wysokie 4 | **Prawdopodobieństwo** |

| Wpływ | Prawdopodobieństwo | Istotność |
|---|---|---|

| | | ( funkcja wpływu i prawdopodobieństwa ) |
|---|---|---|
| 1 – niski<br>2 – średni<br>3 – wysoki<br>4 – bardzo wysoki | 1 – niskie<br>2 – średnie<br>3 – wysokie<br>4 – bardzo wysokie | Nieznaczna 1 - 4<br>Umiarkowana 5 – 8<br>Wysoka 9 -11<br>Poważna 12 -16 |

Ocena ryzyka umożliwia oszacowanie i hierarchizację ryzyka.

Dla oceny istotności ryzyka stosuje się czterostopniową skalę obejmującą następujące poziomy:

1) Poważny – jest to ryzyko o wartości 12–16, które istotnie wpływa na kluczową działalność jednostki, uniemożliwia realizację jej zadań i celów, rodzi straty finansowe,

2) Wysoki – jest to ryzyko o wartości 9 – 11, które potencjalnie wpływa na kluczową działalność jednostki, jest zagrożeniem dla realizacji zadań i celów, zagraża powstaniem strat finansowych,

3) Umiarkowany – jest to ryzyko o wartości 5 – 8, które nie ma zasadniczego wpływu na kluczową działalność jednostki, nie uniemożliwia realizacji zadań i osiągania celów

4) Nieznaczny – jest to ryzyko o wartości 1 - 4, które nie wpływa na kluczową działalność jednostki, nie uniemożliwia realizacji zadań i osiągania celów, podlega minimalnemu monitorowaniu.

**Skala dopuszczalności ryzyka:**

| **Oszacowanie ryzyka** | **Dopuszczalność ryzyka** | **Działania** |
|---|---|---|
| Ryzyko poważne<br>Skala: 12 - 16 pkt | Niedopuszczalne (nieakceptowalne) | Zaleca się rozważenie możliwości przeniesienia ryzyka na inny podmiot lub jeśli to możliwe wycofanie się z realizacji zadania powodującego ryzyko do czasu zmniejszenia ryzyka do poziomu dopuszczalnego. |
| Ryzyko wysokie<br>Skala: 9 – 11 pkt | Niedopuszczalne (nieakceptowalne) | Zaleca się zaplanowanie i podjęcie działań, których celem jest zdecydowane zmniejszenie ryzyka |
| Ryzyko umiarkowane<br>Skala: 5 - 8 pkt | Dopuszczalne (akceptowalne) | Zaleca się zaplanowanie i podjęcie działań, których celem jest zdecydowane i skuteczne zmniejszenie ryzyka |
| Ryzyko nieznaczne<br>Skala: 1 – 4 pkt | Dopuszczalne (akceptowalne) | Zaleca się rozważenie możliwości dalszego zmniejszenia poziomu ryzyka lub zapewnienie, że ryzyko pozostanie na tym samym poziomie |

……..

(podpis Administratora Danych – Kierownika Jednostki)

# ARKUSZ SZACOWANIA RYZYKA OCHRONY DANYCH OSOBOWYCH W OŚRODKU POMOCY SPOŁECZNEJ W STARYM SĄCZU

| *1* | *2* | *3* | *4* | *5* | *6* | *7* | *8* | *9* | *10* |
|---|---|---|---|---|---|---|---|---|---|
| *Lp.* | *Proces / nazwa czynności przetwarzania ( zgodnie z RCPDO )* | *Ryzyko* | *Prawdopodobieństwo* wystąpienia ryzyka (skala 1-4 pkt)* | *Skutek** (skala 1-4 pkt)* | *Poziom wpływu ryzyka na bezpieczeństwo (Istotność ryzyka)*** (skala 1-16 pkt, mnożymy kolumny 4 i 5)* | *Ocena ryzyka – wynik (dopuszczalność)* | *Istniejące mechanizmy kontroli, przeciwdziałania ryzyku* | *Propozycje reakcji na ryzyko* | *Właściciel ryzyka* |
| 1 | | | | | | | | | |
| | | *(dodać kolejne wiersze w razie potrzeby)* | | | | | | | |

LEGENDA

* Sposób oceny prawdopodobieństwa wystąpienia ryzyka

| Prawdopodobieństwo wystąpienia ryzyka | Ilość punktów | Przesłanki |
|---|---|---|
| Bardzo wysokie (81-100%) | **4** | Przewiduje się, że zdarzenie z pewnością wystąpi w ciągu roku |
| Wysokie (61-80%) | **3** | Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się wielokrotnie w ciągu roku |
| Średnie (21-60%) | **2** | Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się raz lub kilka razy w ciągu roku |
| Niskie (0-20%) | **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 |
|---|---|---|
| Bardzo wysoki | 4 | Poważna niezgodność z przepisami prawa. Brak procedur dla danego procesu. Olbrzymie zakłócenia pracy. Znaczny uszczerbek na wizerunku. Zagrożenia spowodują brak zachowania ciągłości procesów działania, utrzymania funkcjonalności systemów niezbędnych do wykonywania podstawowych celów. Brak osiągnięcia kluczowych celów. Straty finansowe. |
| Wysoki | 3 | Duże zagrożenie realizacji kluczowych zadań albo osiągania założonych celów. 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 |

***Skala dopuszczalności ryzyka:

| Oszacowanie ryzyka | Dopuszczalność ryzyka | Działania |
|---|---|---|
| Ryzyko poważne Skala: 12 - 16 pkt. | Niedopuszczalne (nieakceptowane) | Zaleca się rozważenie możliwości przeniesienia ryzyka na inny podmiot lub jeśli to możliwe wycofanie się z realizacji zadania powodującego ryzyko do czasu zmniejszenia ryzyka do poziomu dopuszczalnego. |
| Ryzyko wysokie Skala: 9 – 11 pkt. | Niedopuszczalne (nieakceptowane) | Zaleca się zaplanowanie i podjęcie działań ,których celem jest zdecydowane zmniejszenie ryzyka |
| Ryzyko umiarkowane Skala: 5 - 8 pkt | Dopuszczalne (akceptowane) | Zaleca się zaplanowanie i podjęcie działań ,których celem jest zdecydowane i skuteczne zmniejszenie ryzyka |
| Ryzyko nieznaczne Skala: 1- 4 pkt | Dopuszczalne (akceptowane) | Zaleca się rozważenie możliwości dalszego zmniejszenia poziomu ryzyka lub zapewnienie, że ryzyko pozostanie na tym samym poziomie |