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	Czynności wymienione w kolumnie 1 wiersze 1-25 w RCPDO Ośrodka - załącznik nr 2 Zarządzenia Nr 13/2022 Kierownika Ośrodka Pomocy Społecznej w Starym Sączu z dnia 28 grudnia 2022 r.	Nieuprawniony dostęp do pomieszczenia, w którym są przetwarzane dane osobowe	1	2	2	Dopuszczalne (akceptowane)	Obsługa klientów Ośrodka odbywa się w ściśle określonych miejscach	Działanie: niedopuszczanie osób postronnych do pomieszczeń gdzie przetwarzane są DO	pracownicy administracyjni Ośrodka
		Ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe	1	2	2	Dopuszczalne (akceptowane)	wyznaczony pracownik co miesiąc spisuje na liście zmianę haseł, do listy nie ma dostępu nikt postronny	Działanie, łagodzenie: przypominanie pracownikom o obowiązku zmiany haseł, chronienia haseł, unikatowości haseł	pracownicy administracyjni Ośrodka
		Nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik	1	1	1	Dopuszczalne (akceptowane)	Nie stosuje się cyfrowych nośników danych (pendrivy, płyty CD/DVD)	Działanie, łagodzenie: przypominanie pracownikom o ww. zakazie	pracownicy administracyjni Ośrodka
		Utrata nośnika zawierającego dane osobowe	1	1	1	Dopuszczalne (akceptowane)	Komputery, serwery (nośniki danych) nie są wynoszone poza budynek Ośrodka	Działanie, łagodzenie: przypominanie pracownikom o ww. zakazie	pracownicy administracyjni Ośrodka
		Atak wirusa	2	2	4	Dopuszczalne (akceptowane)	programy antywirusowe są nabywane u sprawdzonych dostawców i na bieżąco aktualizowane	Działanie, łagodzenie: przypominanie pracownikom o zakazie wyłączania programu antywirusowego, zgłaszania niepokojących komunikatów	pracownicy administracyjni Ośrodka
		Klęska żywiołowa, wypadek, zdarzenie losowe, pożar, powódź	1	1	1	Dopuszczalne (akceptowane)	Budynek Ośrodka posiada odpowiednie zabezpieczenia, konstrukcja stosunkowo nowa, wyposażona w instalację odgromową. Przeglądy techniczne prowadzone na bieżąco według zaleceń	Działanie, łagodzenie: przypominanie pracownikom o przestrzeganiu zasad i instrukcji BHP, właściwej i bezpiecznej obsłudze sprzętu elektronicznego, instalacji elektrycznej etc.	pracownicy administracyjni Ośrodka
		Włamanie do systemu komputerowego	1	1	1	Dopuszczalne (akceptowane)	Wprowadzona polityka haseł (co miesięczna ich zmiana do systemu operacyjnego jak również programów dziedzinowych. Programy antywirusowe	Działanie, łagodzenie: przypominanie pracownikom o właściwym zabezpieczeniu stanowiska po pracy, w jej trakcie (wygaszacze ekranu/ systemu z koniecznością ponownego logowania po opuszczaniu stanowiska	pracownicy administracyjni Ośrodka
		Błędy i pomyłki pracowników	1	1	1	Dopuszczalne (akceptowane)	Ośrodek zapewnia szkolenia merytoryczne, spotkania pracownicze	Działanie, łagodzenie: Motywowanie pracowników do	pracownicy administracyjni

							podczas których omawia się bieżące problemy	dalszego doskonalenia warsztatu pracy, zgłaszaniu uwag/sugestii podnoszących standard pracy	Ośrodka	
		Awaria sprzętu	1	1	1	Dopuszczalne (akceptowane)	Sprzęt jest wymieniany/naprawiany według bieżących potrzeb	Działanie, łagodzenie: przypominanie pracownikom o użytkowaniu sprzętu zgodnie z przeznaczeniem i zgłaszaniu ewentualnych awarii	pracownicy administracyjni Ośrodka	
		Brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania	1	1	1	Dopuszczalne (akceptowane)	Pracownicy są zobowiązani do zabierania dokumentów zaraz po ich wydruku/kopiowaniu z urządzeń. Sprzęt wielofunkcyjny nie jest dostępny dla osób postronnych	Działanie, łagodzenie: przypominanie pracownikom o ww. obowiązku	pracownicy administracyjni Ośrodka	
		Nieuprawnione wprowadzenie zmian w treści dokumentu zawierającego dane osobowe	1	1	1	Dopuszczalne (akceptowane)	W Ośrodku stosuje się unikatowe loginy, które określają który pracownik wykonywał dany etap pracy	Działanie, łagodzenie: przypominanie pracownikom o obowiązku przestrzegania pracy w ramiach udzielonych upoważnień i kompetencji	pracownicy administracyjni Ośrodka	

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

Stary Sącz, luty 2023