Załącznik Nr 4 do
Polityki Bezpieczeństwa Danych Osobowych
Miejskiego Ośrodka Sportu i Rekreacji w Lubartowie

A N A L I Z A R Y Z Y K A

(aktualizacja – wrzesień 2023 roku)

dla danych osobowych przetwarzanych w Miejskim Ośrodku Sportu i Rekreacji w Lubartowie

1. Podstawy prawne opracowania przedmiotowego dokumentu

Art. 24, 25, 32 Rozporządzenia 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 (Dz. Urz. UE L119 z 4 maja 2016 r.).

2. Podstawowe pojęcia

Ryzyko – wpływ czynników wewnętrznych oraz zewnętrznych, które mogą spowodować naruszenie bezpieczeństwa, prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia, nieuprawnionego dostępu do danych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Zagrożenie – potencjalne zdarzenie/naruszenie/niepożądany incydent.

Skutki – rezultaty następstwa niepożądanego incydentu (straty w przypadku wystąpienia zagrożenia). Ocena następstw i wystąpienia ryzyka polega na oszacowaniu potencjalnych skutków, których zaistnienie może wywrzeć negatywny wpływ na osiągnięcie celów.

Analiza ryzyka – określone działania skierowane na obniżenie negatywnego wpływu ryzyka na funkcjonowanie danego podmiotu i podejmowanie odpowiednich działań służących przeciwdziałaniu i ograniczaniu ryzyka. Pozwala na identyfikację, ocenę i monitorowanie poziomu ryzyka w sposób jakościowy i ilościowy, najczęściej przy wykorzystywaniu odchylenia standardowego i współczynnika zmienności.

Szacowanie ryzyka – -jest to całościowy proces analizy i oceny ryzyka.

Ocena ryzyka – proces porównania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia tegoż ryzyka.

Zarządzanie ryzykiem – to proces identyfikacji, oceny, postępowania i kontroli potencjalnych zdarzeń lub sytuacji, dostarczający racjonalnego zapewnienia, ze cele organizacji zostaną zrealizowane.

Bezpieczeństwo danych osobowych – zapewnienie poufności, dostępności i integralności, ale również inne właściwości takie jak autentyczność, rozliczalność.

Dostępność – właściwość określająca niczym nie ograniczoną możliwość wykorzystania zasobu na żądanie w określonym czasie przez uprawnioną osobę.

Integralność – należy przez to rozumieć właściwość określającą, że zasób/aktywa nie został zmodyfikowany w sposób nieuprawniony.

Poufność – należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym.

Zasób – osoby, usługi, oprogramowanie, sprzęt oraz inne elementy mające wpływ na bezpieczeństwo przetwarzanych danych osobowych.

3. Źródła zagrożenia

Źródła zagrożeń dla przetwarzanych danych osobowych mogą stanowić:

1) **siły natury** – zdarzenia, które nie wynikają z działalności człowieka, tzn.

uderzenie pioruna, pożar będący konsekwencją ww. uderzenia pioruna, powódź, zalanie, starzenie się sprzętu, nośników pamięci, kurz, katastrofa budowlana, ulewny deszcz, ekstremalne temperatury;

2) **ludzie** – mogą to być pracownicy lub osoby z zewnątrz działający w sposób celowy lub przypadkowy. Zagrożenia te to przede wszystkim: błędy i pomyłki użytkowników, administrujących danymi, osób upoważnionych, zaniedbania podczas przesyłania, udostępniania, kopiowania, zagubienie nośnika, niewłaściwe zniszczenie, nielegalne użycie, brak osób upoważnionych do dostępu do danych, podpalenie obiektu zalanie wodą, sabotaż, zmiany napięcia w sieci, niedobór pracowników, kradzież, włamanie do systemu, wyłudzenie, fałszowanie dokumentów, podszycie się pod osobę upoważnioną.

4. Analiza ryzyka

Analiza ryzyka polega na identyfikacji podatności zasobów na wyselekcjonowane zagrożenia oraz oszacowanie skutków utraty bądź ujawnienia informacji stanowiących dane osobowe **Miejskiego Ośrodka Sportu i Rekreacji w Lubartowie**. Celem przeprowadzonej analizy ryzyka jest dostarczenie informacji do podjęcia decyzji w zakresie przeciwdziałania zagrożeniom i zmniejszania podatności na poszczególne zagrożenia. Zgodnie z metodyką dla każdego zidentyfikowanego zagrożenia zostały przypisane poziomy podatności zasobów na zagrożenia. Podatność określa łatwość wyrządzenia szkody dla wskazanego zasobu w kontekście utraty poufności, integralności i dostępności.

1) **Podatność na zagrożenia.** Poziom skutku oraz podatności na zagrożenia zasobów w każdej kategorii przedstawia się następująco:
1.a) Brak (0);
1.b) Niski (1-4);
1.c) Średni (5-7);
1.d) Wysoki (8-9);
1.e) Ekstremalny (10).

2) **Wagi.** Dla poszczególnych wartości ryzyka przyjmuje się następujące wagi:
2.a) **ryzyko bardzo niskie 1-19 pkt**; (poziom ryzyka akceptowalny – pomijalny);
2.b) **ryzyko niskie 20-29 pkt;** (poziom ryzyka akceptowalny – działania podejmowane w zależności od wymaganych nakładów);
2.c) **ryzyko średnie 30-39 pkt;** (poziom ryzyka nieakceptowalny – działanie może zostać przesunięte w czasie ale wymaga okresowego monitorowania);
2.d) **ryzyko wysokie 40-49 pkt;** (poziom ryzyka nieakceptowalny – działanie może zostać przesunięte w czasie ale wymaga stałego monitorowania);
2.e) **ryzyko maksymalne powyżej 50 pkt.** (poziom ryzyka nietolerowany – wymaga natychmiastowego działania).

Tabelaryczne zestawienie zidentyfikowanych zagrożeń dla przetwarzanych danych osobowych w Miejskim Ośrodku Sportu i Rekreacji w Lubartowie

W kolumnie *„Skutki"* określa się wpływ, jaki konkretne zagrożenie będzie miało na dany zasób. Wyznacza się go poprzez przypisanie umownej wartości liczbowej z zakresu 1-10 na podstawie wiedzy i doświadczeń osób prowadzących szacowanie. Następnie określana jest podatność rozumiana jako prawdopodobieństwo urzeczywistnienia określonego zagrożenia poprzez nadanie wartości w skali 1-10.

Miara ryzyka jest iloczynem wartości określonych dla skutku zagrożenia i podatności zasobu na zagrożenie.

Zasoby	**Stanowiska komputerowe**								
Zagrożenia	**Poufność**			**Dostępność**			**Integralność**		
	Skutki (S)	Podatność (P)	Ryzyko (R)=P*S	Skutki (S)	Podatność (P)	Ryzyko (R)=P*S	Skutki (S)	Podatność (P)	Ryzyko (R)=P*S
Sprzęt (stanowiska komputerowe)									
Nieuprawnione wykonanie kopii danych z dysku lub nośnika	7	4	28	5	4	20	7	4	28
Korzystanie z nielicencjonowanego oprogramowania	3	4	12	5	2	10	6	2	12
Uszkodzenie stanowiska	4	2	8	10	2	20	10	2	20
Uszkodzenie nośnika	8	2	16	9	2	18	9	2	18
Wykorzystanie cudzych danych do autoryzacji	9	2	18	9	2	18	9	2	18
Informatyczne nośniki danych									
Zagubienie nośnika	10	2	20	9	2	18	10	2	20
Nieuprawnione wynoszenie nośnika poza obszar	8	2	16	8	2	16	8	2	16
Nieuprawnione usuniecie danych	2	1	2	10	2	20	10	2	20
Nieuprawniony dostęp do nośników	10	2	20	10	2	20	10	2	20

Zasoby	**Konfiguracja systemu**								
Zagrożenia	**Poufność**			**Dostępność**			**Integralność**		
	Skutki (S)	Podatność (P)	Ryzyko (R)=P*S	Skutki (S)	Podatność (P)	Ryzyko (R)=P*S	Skutki (S)	Podatność (P)	Ryzyko (R)=P*S
Awarie i zakłócenia w pracy stanowiska komputerowego									
Uszkodzenie techniczne stanowiska komputerowego	8	2	16	9	2	18	9	2	18
Awaria oprogramowania	8	2	16	10	2	20	10	2	20
Brak zasilania	3	2	6	9	2	18	3	2	6
Brak możliwości zalogowania się	4	2	8	9	2	18	3	2	6

Nieznajomość hasła użytkownika	4	1	4	10	2	20	3	1	3
Ataki, włamania do systemu									
Przełamanie mechanizmów dostępu	10	2	20	9	2	18	10	2	20
Instalacja i użytkowanie złośliwego oprogramowania	10	2	20	9	2	18	10	2	20
Ataki hackerskie	9	2	18	8	2	16	9	2	18
Administrowanie systemem									
Brak odpowiednio przeszkolonych administratorów	10	4	40	10	4	40	10	4	40
Błędy i pomyłki w zarządzaniu systemem	6	4	24	6	4	24	6	4	24
Ujawnienie hasła administratora	8	2	16	8	2	16	8	2	16
Rutyna i/ lub nadmiar obowiązków administratora	8	3	24	8	3	24	6	3	18
Brak ciągłości w zarządzaniu kontami użytkowników,(terminowe zakładanie i likwidacja)	7	4	28	7	4	28	7	4	28

Zasoby	**Pomieszczenia i budynki**								
Zagrożenia	**Poufność**			**Dostępność**			**Integralność**		
	Skutki (S)	Podatność (P)	Ryzyko (R)= P*S	Skutki (S)	Podatność (P)	Ryzyko (R)= P*S	Skutki (S)	Podatność (P)	Ryzyko (R)=P*S
Brak dostępu do pomieszczenia	3	1	3	8	2	16	8	2	16
Dokumenty									
Nieuprawniony dostęp do dokumentów	9	3	27	9	3	27	9	3	27
Kradzież dokumentów	9	3	27	9	3	27	9	3	27
Przypadkowe zniszczenie lub utrata dokumentów	7	3	21	9	3	27	9	3	27
Zagubienie dokumentów	7	4	28	7	4	28	7	4	28
Nieuprawnione wynoszenie dokumentu poza obszar przetwarzania	7	4	28	7	4	28	7	4	28
Brak aktualizacji procedur przetwarzania danych osobowych (polityk, instrukcji itp.)	5	3	15	3	2	6	5	3	15
Klęska żywiołowa i katastrofy									
Pożar	5	5	25	5	5	25	5	5	25
Powódź/zalanie	5	5	25	5	5	25	5	5	25

Piorun	7	2	14	10	2	20	10	2	20
Katastrofy budowlane	7	2	14	10	2	20	10	2	20
Kurz i zanieczyszczenia	3	2	6	10	2	20	10	2	20

Zasoby	**Zasoby ludzkie**								
Zagrożenia	**Poufność**			**Dostępność**			**Integralność**		
	Skutki (S)	Podatność (P)	Ryzyko (R)= P*S	Skutki (S)	Podatność (P)	Ryzyko (R)= P*S	Skutki (S)	Podatność (P)	Ryzyko (R)=P*S
Brak odpowiednio przeszkolonych użytkowników	9	3	27	9	3	27	9	3	27
Zbieranie danych osobowych bez podstawy prawnej	10	2	20	10	2	20	10	2	20
Nieprzestrzeganie praw osób, których dane dotyczą	10	2	20	10	2	20	10	2	20
Rutyna i /lub nadmiar obowiązków użytkownika	10	2	20	10	2	20	10	2	20
Zaniedbania ze strony personelu obsługującego proces przetwarzania danych	10	2	20	10	2	20	10	2	20
Przetwarzanie danych przez osoby nie posiadających upoważnień	9	3	27	9	3	27	9	3	27
Nieprzestrzeganie procedur przetwarzania danych osobowych	8	3	24	5	5	25	5	5	25
Brak nadzoru przełożonych	6	4	24	7	4	28	6	4	24

5. Ocena ryzyka

OCENA RYZYKA

Maksymalny poziom ryzyka określono jako **40** co mieści się w przedziale **ryzyka wysokiego 40 – 49 pkt.** (poziom ryzyka nieakceptowalny – działanie może zostać przesunięte w czasie ale wymaga stałego monitorowania).

Oznacza to, iż zastosowane środki techniczne i organizacyjne stosowane w **Miejskim Ośrodku Sportu i Rekreacji w Lubartowie** nie zapewniają wymaganego stopnia bezpieczeństwa przetwarzania danych osobowych w zakresie możliwości wystąpienia zagrożeń wynikających z **braku odpowiednio przeszkolonych administratorów – ryzyko wysokie 40.**

Z powyższego wynika, iż MOSIR w Lubartowie **nie w pełni zapewnia stopień** bezpieczeństwa odpowiadający temu ryzyku oraz nie uwzględnia w dostatecznym stopniu ryzyka naruszenia praw i wolności osób fizycznych, których dane dotyczą.

POSTĘPOWANIE Z RYZYKIEM

W wyniku oceny przedstawionych wyżej ryzyk przyjmuje się, iż dla uzyskania redukcji poziomu ryzyka do poziomu akceptowalnego, istnieje konieczność przeprowadzania następujących działań o charakterze organizacyjnym i technicznym:

1) nawiązanie współpracy z osobą lub podmiotem przeszkolonym w zakresie realizacji zadań Administratora Systemów Informatycznych,
2) podnoszenie świadomości pracowników poprzez szkolenia dotyczące bezpieczeństwa przetwarzania danych,
3) aktualizacja oprogramowania systemowego oraz zabezpieczającego wyłącznie przez Administratora Systemu Informatycznego oraz stały nadzór ASI nad konfiguracją i aktualizacją oprogramowania odpowiadającemu za bezpieczeństwo danych.

W pozostałym zakresie **oszacowane obecnie ryzyka uznaje się za niskie i możliwe do akceptacji** pod kątem możliwości wystąpienia naruszeń praw i wolności osób, których dane dotyczą.

Administrator akceptuje ryzyka zawarte w tabeli szacowania ryzyk na poziomie niskim, natomiast dla ryzyk na poziomie wysokim podejmie wskazane wyżej działania mające na celu ich redukcję.

Niezbędne jest dalsze monitorowanie wszystkich zagrożeń wykazanych w niniejszej analizie. Wszelkie przyszłe zmiany dotyczące procesów przetwarzania danych osobowych oraz ewentualne wystąpienia naruszeń ochrony danych będą powodowały konieczność ponownego szacowania ryzyk i mogą wykazać, że niezbędne jest podjęcie dodatkowych działań mających na celu ich redukcję.

Administrator akceptuje ustalenia niniejszej analizy poprzez sygnowanie jej podpisem.

Akceptuję wyniki analizy ryzyka

Dyrektor
Miejskiego Ośrodka
Sportu i Rekreacji
w Lubartowie
mgr Andrzej Sambor

.....
(Data i podpis Administratora Danych Osobowych)