Polityka Ochrony Danych Osobowych

w

Ośrodku Kultury w Mirosławcu

OŚRODEK KULTURY W MIROSŁAWCU

1 WSTĘP

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia
27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

2 ANALIZA RYZYKA

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania.

2.1 DEFINICJE

1. **Aktywa** – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych.
2. **Naruszenie (Incydent) ochrony danych osobowych** - to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. **Zagrożenie** - potencjalne naruszenie (potencjalny incydent).
4. **Skutki** - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia).
5. **Ryzyko** - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie aktywów.

2.2 REJESTR CZYNNOŚCI PRZETWARZANIA (INWENTARYZACJA DANYCH OSOBOWYCH)

Administrator będący równocześnie w stosunku do niektórych zbiorów Podmiotem przetwarzającym jest zobowiązany zgodnie z art. 30 RODO do prowadzenia rejestru czynności przetwarzania. Rejestr stanowi podstawę do przeprowadzenia analizy ryzyka.

1. Administrator prowadzi rejestr zgodnie z Załącznikiem nr 1 - Rejestr czynności przetwarzania (wykaz zbiorów danych osobowych).
2. Podmiot przetwarzający prowadzi rejestr zgodnie z Załącznikiem nr 2 - Rejestr czynności prowadzony przez Podmiot przetwarzający.

2.3 Wyznaczenie zagrożeń

1. Administrator jest odpowiedzialny za określenie listy zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić podczas przetwarzania danych osobowych.
2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zinwentaryzowanych zbiorów (kategorii osób), aktywów oraz procesów przetwarzania.

2.4 Wyliczenie ryzyka dla zagrożeń

1. Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze (dla kategorii osób) lub w procesie przetwarzania.
2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A.
3. Administrator określa Skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne.
4. Proponowaną Skalę skutków prezentuje Tabela B.
5. Administrator wylicza Ryzyka (**R**) dla wszystkich zagrożeń i ich skutków w/g formuły: **R = P * S.**

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
małe (do 10000 PLN, incydent prasowy lokalny)	1
średnie (10000-100000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100000 PLN, naruszenie prawa)	3

2.4.1 Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem.
2. Proponowaną skalę Ryzyka prezentuje Tabela C.

Tabela C POZIOM RYZYKA	**WARTOŚĆ [R = P*S]**
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

2.4.2 Reakcja na wartość ryzyka

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń.
2. Działania obniżające ryzyko, które może zastosować Administrator:

a. Przeniesienie –przerzucenie ryzyka (outsourcing, ubezpieczenie),
b. Unikanie – eliminacja działań powodujących ryzyko.

3. Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka.
4. Analizę ryzyka przeprowadza się w specjalnym szablonie stanowiącym Załącznik nr 3 - Arkusz analizy ryzyka RODO natomiast stosowane zabezpieczenia wykazano w Załączniku nr 3a – Wykaz zabezpieczeń RODO.

2.4.3 Ponowna analiza ryzyka

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne).

2.5 Plan postępowania z ryzykiem

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne, patrz Załącznik nr 4 - Plan postępowania z ryzykiem.
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

3 Upoważnienia

1. Administrator/podmiot przetwarzający odpowiada za nadawanie/anulowanie upoważnień do przetwarzania danych w zbiorach w postaci papierowej oraz w systemach informatycznych.
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.
3. Upoważnienia nadawane są do zbiorów na wniosek przełożonych osób, zgodnie z zakresem obowiązków. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie – patrz Załącznik nr 5 - Upoważnienie do przetwarzania danych osobowych.
4. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Patrz Załącznik nr 6 - Ewidencja osób upoważnionych.
5. W przypadku powierzenia przetwarzania danych do Podmiotu przetwarzającego, Administrator jest zobowiązany do sporządzenia z nim umowy powierzenia, stanowiącą podstawę upoważnienia dla osób z Podmiotu przetwarzającego - patrz Załącznik nr 7 - Umowa powierzenia.
6. Administrator prowadzi ewidencję umów powierzenia według Załącznika nr 8 – Rejestr umów powierzenia.

4 Środki techniczne i organizacyjne zabezpieczające dane osobowe

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych, patrz Załącznik nr 9 - Instrukcja zarządzania RODO.
2. W instrukcji wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne.
3. Instrukcja jest aktualizowana, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka.
4. Administrator opracował Politykę kluczy, która stanowi Załącznik nr 10 – Polityka kluczy.

5 REGULAMIN OCHRONY DANYCH OSOBOWYCH

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. Patrz Załącznik nr 11 - Regulamin Ochrony Danych Osobowych.

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania poprzez podpisanie oświadczenia o poufności stanowiącego Załącznik nr 12 – Oświadczenie o poufności.

6 INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów. bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego (lub jeśli jest powołany – Inspektora Ochrony Danych).
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą
    i utratą danych osobowych,
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników
    (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
4. W przypadku stwierdzenia wystąpienia incydentu, Administrator (lub w przypadku powołania – IOD) prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,
    b. inicjuje ewentualne działania dyscyplinarne,
    c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu,
    d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych, incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze –patrz Załacznik nr 13 - Formularz rejestracji incydentu.
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.