Polityka Ochrony Danych Osobowych w Miejskim Ośrodku Kultury i Bibliotece w Piławie Górnej

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.

Przy opracowaniu Polityki uwzględniono również zapisy zawarte w ustawie z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jedn. Dz.U. z 2014 r. poz. 1114 ze zm.) i w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2016 r., poz. 113).

2. OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH, FORMA, PRZEPŁYWY

Obszar przetwarzania danych osobowych w Miejskim Ośrodku Kultury i Bibliotece w Piławie Górnej obejmuje siedzibę Miejskiego ośrodka Kultury i Biblioteki, tj. budynek Miejskiego Ośrodka Kultury położony w Piławie Górnej, ul. Piastowskiej 40 oraz budynek Biblioteki przy ul. Sienkiewicza 32, pomieszczenia i części pomieszczeń Miejskiego Ośrodka Kultury i Biblioteki, w których przetwarzane są dane osobowe (miejsca, w których wykonuje się operacje na danych osobowych, tj. wpisuje, zmienia, kopiuje), oraz miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające elektroniczne nośniki informacji, pomieszczenia, w których składowane są uszkodzone nośniki danych).

Warunki ochrony obszaru przetwarzania danych osobowych określone zostały w Załączniku nr 1 do Polityki **„Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe".**

Obszar przetwarzania danych osobowych określony jest w **„Wykazie pomieszczeń, w których przetwarzane są dane osobowe".** Wzór wykazu stanowi Załącznik nr 2 do Polityki.

Przetwarzanie danych osobowych w zbiorach danych odbywa się w formie papierowej i elektronicznej. Przetwarzanie danych osobowych w formie elektronicznej odbywa się na serwerze i na stacjach roboczych użytkowników.

W ramach procesów przetwarzania danych ma miejsce przepływ danych pomiędzy różnymi systemami informatycznymi. Informacje na temat przepływu danych pomiędzy różnymi systemami informatycznymi znajdują się w **„Rejestrze czynności przetwarzania",** (RCP) o którym mowa w podrozdziale 3.2. - Załącznik nr 3.

Szczegółowe informacje dotyczące przepływu danych osobowych pomiędzy danymi systemami informatycznymi znajdują się w instrukcjach zarządzania danym systemem.

3. 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.

3.1 DEFINICJE

Użyte w niniejszej Polityce pojęcia są wspólne dla wszystkich dokumentów powiązanych z Polityką oraz dla wszystkich pozostałych dokumentów, które zostały przyjęte przez GBP w zakresie ochrony danych osobowych.

1. **Administrator (danych)** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W Miejskim Ośrodku Kultury i Bibliotece w Piławie Górnej, dalej zwanym MOKiB, Administratorem Danych Osobowych jest MOKiB reprezentowany przez Dyrektora jednostki.

2. **RODO** – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016).
3. **Dane osobowe** - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego opisującego tożsamość tej osoby fizycznej.
4. **Przetwarzanie danych osobowych** to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.
5. **Ograniczenie przetwarzania** - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
6. **Anonimizacja**- zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych.
7. **Zgoda osoby, której dane dotyczą** - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.
8. **Ocena skutków w ochronie danych -** to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.
9. **Podmiotem danych** jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.
10. **Odbiorca** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.
11. **Podmiot przetwarzający** (**Procesor)** to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.
12. **Inspektor Ochrony Danych (IODO) -** to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.
13. **Pseudonimizacja -** oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. Listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
14. **Szczególne kategorie danych osobowych** - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życia seksualnego osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.
15. **Profilowanie** – jest dowolną formą zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

16. **Naruszenie ochrony danych osobowych -** jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, wszelkiego zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu (włamania) do danych osobowych. W szczególności oznacza nieujawniony dostęp lub próbę dostępu do danych przetwarzanych w formie informatycznej lub papierowej lub pomieszczeń, w których się one znajdują, naruszenie lub próby naruszania integralności systemu, poufności danych lub ich części. Zniszczenie, uszkodzenie lub wszelką ingerencję w systemy informatyczne zmierzające do zakłócenia ich działania bądź pozyskania w sposób niedozwolony danych zawartych w systemach informatycznych lub poza nimi.

3.2 REJESTR CZYNNOŚCI PRZETWARZANIA (RCP) - INWENTARYZACJA DANYCH OSOBOWYCH

Administrator jest zobowiązany zgodnie z art. 30 RODO do prowadzenia rejestru czynności przetwarzania.
Rejestr stanowi podstawę do przeprowadzenia analizy ryzyka.
Administrator prowadzi rejestr zgodnie z Załącznikiem nr 3 **„Rejestr czynności przetwarzania".**

3.3 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.

3.4 WYLICZENIE RYZYKA DLA ZAGROŻEŃ

1. Administrator określa Prawdopodobieństwo (**P**) wystąpienia (wedle parametrów poufności, dostępności i integralności) 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
zagrożenie pewne	4

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
katastrofalne	4

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 nie występuje	0
ryzyko pomijalne i akceptowalne (akceptujemy)	1 – 3
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	4 – 6
ryzyko jest nieakceptowalne (musimy obniżyć)	7 – 16

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 **„Analiza oceny ryzyka”** - Załącznik nr 4.

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).

3.5 PLAN POSTĘPOWANIA Z RYZYKIEM

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne, patrz **Plan redukcji ryzyka** – Załącznik nr 4a
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

4. ZARZĄDZANIE PRZETWARZANIEM DANYCH / UPOWAŻNIENIA

1. Obowiązki ADO zostały określone w RODO i wydanych na jego podstawie przepisach krajowych.
2. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach (dla kategorii osób) w postaci papierowej oraz w systemach informatycznych.
3. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.
4. Upoważnienia nadawane są do zbiorów (dla kategorii osób) na wniosek przełożonych osób. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie – patrz Załącznik nr 5 **„Upoważnienie do przetwarzania danych osobowych”.**
5. Administrator prowadzi rejestr osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencja ma charakter pomocniczy i nie jest wymagana przepisami RODO. Patrz Załącznik nr 6 **„Rejestr upoważnień”.**
6. 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 uniwersalna**”. Ewidencja umów powierzenia jest prowadzona w **Rejestrze umów powierzenia** – Załącznik nr 8.
7. ADO wyznacza Inspektora Ochrony Danych Osobowych (IODO) oraz osobę odpowiedzialną (Informatyk) za zabezpieczenie technologiczne przetwarzania danych osobowych.
8. Obowiązki IODO zostały określone w RODO. W szczególności do obowiązków IODO należy:

a. informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
b. monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
c. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
d. współpraca z organem nadzorczym;
e. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

9. Informatyk (dopuszczalna umowa zlecenie z zewnętrznym wykonawcą) odpowiada za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych MOKiB.
10. Administrator pełni rolę zarządzającego oprogramowaniem w MOKiB. Natomiast informatyk przeprowadza okresową inwentaryzację oprogramowania oraz ustanawia zasady i procedury ciągłego utrzymania oprogramowania.
11. W procesie przetwarzania danych osobowych uczestniczy każdy pracownik MOKiB i powinien przestrzegać zasad przetwarzania i ochrony danych osobowych przetwarzanych w MOKiB. Każda upoważniona do przetwarzania danych osoba jest osobiście odpowiedzialna za bezpieczeństwo powierzonych jej danych.
12. ADO zobowiązany jest ponadto:
    a. zarządzanie zasobem danych osobowych;
    b. nadanie upoważnień dotyczących dostępu do zasobu danych osobowych podległym pracownikom i dla siebie;
    c. zgłaszanie do IODO każdej nowej czynności przetwarzania danych osobowych oraz informacji dotyczących zmian w zakresie i sposobach przetwarzania tego zbioru;
    d. udostępnianie danych osobowych innemu podmiotowi lub osobie, której dane dotyczą;
    e. przestrzeganie obowiązków dotyczących:
        - obszaru przetwarzania,
        - wykazu osób upoważnionych do przetwarzania danych osobowych,
        - stosowania odpowiednich zabezpieczeń zbiorów.
    f. prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych z uwzględnieniem zakresu odpowiedzialności za ochronę tych danych w stopniu odpowiednim do zadań wykonywanych przez te osoby przy przetwarzaniu danych osobowych i przekazywanie IODO aktualnej ewidencji tych osób wraz z priorytetami im przydzielonymi;
    g. zapoznawanie pracowników mających dostęp do danych osobowych z przepisami dotyczącymi ochrony danych osobowych.

14. Dyrektor i pracownicy działów MOKiB , w których są zbieranie i przetwarzane dane osobowe, są odpowiedzialni za poinformowanie osób, których dane osobowe przetwarzają, o ich uprawnieniach wynikających z art. 13 RODO ust. 1 i 2.
15. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy dodatkowo poinformować o źródle danych oraz o uprawnieniach wynikających z art. 14 i art. 15 RODO.

5. PODMIOT PRZETWARZAJĄCY

Powierzenie przetwarzania danych osobowych odbywa się zgodnie z art. 28 i art. 29 RODO na podstawie umowy zawartej na piśmie (draft umowy patrz Załącznik nr 7) pomiędzy ADO a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.

Dyrektor informuje IODO o zamiarze powierzenia danych osobowych do przetwarzania.

IODO przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi.

Projekt umowy opiniują:

- IODO;
- Informatyk – jeżeli zlecenie czynności dotyczyć będzie przetwarzania danych w systemie informatycznym.

6. ŚRODKI TECHNICZNE I ORGANIZACYJNE ZABEZPIECZAJĄCE DANE OSOBOWE / MINIMALIZACJA

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych.
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 dba o minimalizację przetwarzania danych pod kątem: (i) adekwatności danych do celów (ilości danych i zakresu przetwarzania), (ii) dostępu do danych, (iii) czasu przechowywania danych.

Minimalizacja zakresu

Administrator zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

Administrator dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

Administrator przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design*).

Minimalizacja dostępu

Administrator stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe). Administrator stosuje kontrolę dostępu fizycznego.

Administrator dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających, jeżeli takie wystąpi.

Minimalizacja czasu

IODO wdraża mechanizmy kontroli cyklu życia danych osobowych, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w RCP.

Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez MOKiB. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

7. REGULAMIN OCHRONY DANYCH OSOBOWYCH

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. Patrz **„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 zawartego w arkuszu stanowiącym Załącznik nr 5 **„Upoważnienie do przetwarzania danych osobowych".**

8. 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. Niniejsze zapisy stosujemy do danych osobowych przetwarzanych w systemach informatycznych jak i nieinformatycznych czytników papierowych.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu IODO. Zasady postępowania przypadku naruszenia bezpieczeństwa danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych osobowych.
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 należy bezzwłocznie powiadomić IODO. IODO prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;
    b. wysłuchuje relacji osoby która dokonała powiadomienia oraz innych osób związanych z incydentem;
    c. inicjuje ewentualne działania dyscyplinarne;
    d. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu;
    e. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
5. Do czasu przybycia IODO zgłaszający:
    a. powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów;
    b. zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym;
    c. podejmuje stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych;

d. wykonuje polecenia IODO;
e. pracownik może kontynuować pracę dopiero po otrzymaniu pozwolenia przez IODO.

6. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze – patrz Załącznik nr 11 **„Rejestr naruszeń".**
7. IODO po opanowaniu sytuacji nadzwyczajnej opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości. Wzór raportu końcowego stanowi Załącznik nr 10 **„Raport z naruszenia ochrony danych".**
8. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
9. 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.

9. OCENA SKUTKÓW DLA OCHRONY DANYCH

IODO w porozumieniu z Administratorem dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie, tam gdzie mamy do czynienia z systematycznym monitorowaniem na dużą skalę miejsc dostępnych publicznie, zgodnie z art. 35 RODO.