Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych

Miejska i Gminna Biblioteka Publiczna im. ks. Jana Twardowskiego w Strzelinie

ul. Grahama Bella 3a
57-100 Strzelin

Dokument do użytku służbowego.
Wykonał: mgr inż. Piotr Chałaszczyk
- Inspektor Ochrony Danych
Data aktualizacji: 02.11.2020 r.

Spis treści

Wstęp 2

Definicje 2

Wymogi dotyczące bezpieczeństwa danych osobowych 5

Zagrożenia dla systemu ochrony danych osobowych 5

Podatność systemu ochrony danych osobowych na zagrożenia 8

Analiza zagrożeń i szacowanie ryzyka 9

Załączniki 10

Wstęp

Analiza ryzyka jest procesem kluczowym z uwagi na całość systemu bezpieczeństwa danych osobowych. Ma ona na celu ustalenie, jakie są potencjalne zagrożenia związane z przetwarzaniem danych osobowych oraz dobranie zabezpieczeń, które będą najodpowiedniejsze dla Miejskiej i Gminnej Biblioteki Publicznej im. ks. Jana Twardowskiego w Strzelinie.

Administrator Danych Osobowych ze względu na ciążące na nim obowiązki wynikające z przepisów prawa zobowiązany jest do zastosowania środków technicznych i organizacyjnych, które mają zapewnić ochronę przetwarzanych danych osobowych w świetle adekwatnych zagrożeń. Skuteczność zastosowanych środków podlega cyklicznym badaniom. Przy stosowaniu zabezpieczeń uwzględniane są zmieniające się warunki oraz postęp techniczny (informatyczny), co może powodować konieczność zmiany lub modernizowania wprowadzonych wcześniej przez Administratora Danych Osobowych systemów ochrony.

Przy opracowaniu niniejszego dokumentu uwzględniono regulacje zawarte w następujących aktach prawnych:

- Rozporządzeniu 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.
- Wytycznych GIODO pt. „Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych w świetle ogólnego rozporządzenia o ochronie danych osobowych".
- Wytycznych Grupy Roboczej art. 29 dotyczących inspektorów ochrony danych z dn. 13 grudnia 2016 r.
- Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych.

Definicje

Biblioteka, placówka	- Miejska i Gminna Biblioteka Publiczna im. ks. Jana Twardowskiego w Strzelinie.
Administrator Danych Osobowych (ADO)	- osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli sposoby i cele takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony Administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.
Inspektor Ochrony Danych (IOD)	- osoba wyznaczona przez ADO odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę danych osobowych w placówce.

Administrator Systemu Informatycznego (ASI)	- osoba (zespół osób) zatrudniona przez ADO lub współpracująca z ADO, upoważniona do realizacji zadań związanych z zarządzaniem systemem informatycznym.
Użytkownik systemu informatycznego	- osoba upoważniona przez ADO do przetwarzania danych osobowych i zarejestrowana w systemie informatycznym przez Administratora Systemu, która odbyła stosowne szkolenie w zakresie ochrony tych danych.
Osoba upoważniona	- osoba upoważniona przez Administratora Danych Osobowych do przetwarzania danych osobowych w placówce.
Osoba uprawniona	- osoba upoważniona przez Administratora Danych Osobowych do przetwarzania danych osobowych i posiadająca uprawniony przez ADO dostęp do systemu informatycznego, będąca pracownikiem placówki.
Dane osobowe	- informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna, to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
Przetwarzanie danych	- operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
Analiza ryzyka	- systematyczne wykorzystywanie informacji do zidentyfikowania źródeł i oszacowania ryzyka.
Szacowanie ryzyka	- proces oceny i analizy ryzyka.
Ocena ryzyka	- proces porównania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka.
Postępowanie z ryzykiem	- wdrażanie środków modyfikujących ryzyko.

Zarządzanie ryzykiem	- działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka.
Bezpieczeństwo informacji	- zachowanie poufności, integralności i dostępności informacji (dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność).
Zabezpieczenia	- środki o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko.
Zagrożenia	- potencjalna przyczyna niepożądanego zdarzenia, które może wywołać szkodę w zasobach systemu teleinformatycznego.
Podatność	- słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie.
Poufność danych	- właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom i osobom.
Rozliczalność danych	- właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
Integralność danych	- właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
Zagrożenia systemu przetwarzania	- wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę.
Zasoby systemu teleinformatycznego	- informacje przetwarzane w systemie teleinformatycznym, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych informacji.
Incydent związany z bezpieczeństwem informacji	- pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne zakłócenia zadań biznesowych i zagrażają bezpieczeństwu informacji.
Incydent bezpieczeństwa teleinformatycznego	- pojedyncze zdarzenie lub seria zdarzeń związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności.
Informatyczny nośnik danych	- materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej.

Oprogramowanie złośliwe	- oprogramowanie, którego celem jest przeprowadzenie nieuprawnionych lub szkodliwych działań w systemie teleinformatycznym.

Wymogi dotyczące bezpieczeństwa danych osobowych

Bezpieczeństwo przetwarzanych informacji zawierających dane osobowe wymaga:

- zapewnienia ochrony fizycznej stanowisk komputerowych przed nieuprawnionym dostępem,
- ochrony nośników technicznych i wydruków dokumentów, w tym określenia zasad ochrony ich przed nieuprawnionym dostępem,
- zabezpieczenia przed nieupoważnionym dostępem do danych osobowych znajdujących się w zasobach systemu informatycznego,
- zapewnienia dostępności do danych osobowych znajdujących się na technicznych nośnikach informacji oraz w pamięci systemu informatycznego dla upoważnionych użytkowników,
- zapewnienia możliwości kontroli dostępu do zasobów systemu informatycznego oraz wykonywanych na nim czynności,
- zapewnienia możliwości kontroli nośników, na których przetwarzane są dane osobowe.

W celu maksymalnego wyeliminowania zagrożenia dla całego systemu ochrony danych osobowych w bibliotece zostały wdrożone procedury kontrolne, na które składają się:

- prowadzenie odpowiedniej dokumentacji,
- fizyczna ochrona danych osobowych,
- bezpieczne środowisko komputerowe,
- „kodeks dobrych praktyk" wdrożony przez Inspektora OD.

Zagrożenia dla systemu ochrony danych osobowych

System ochrony danych osobowych w Miejskiej i Gminnej Bibliotece Publicznej im. ks. Jana Twardowskiego w Strzelinie narażony jest na zagrożenia wystąpienia incydentu powodującego utratę poufności, rozliczalności i integralności informacji.

Poufność

Poufność, to zapewnienie danym osobowym niemożności ich udostępniania nieupoważnionym osobom czy podmiotom.

Zagrożenia, jakie można wyróżnić ze względu na utratę poufności w systemie:

- klęska żywiołowa, w wyniku której utracono poufność danych osobowych,
- nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są dane osobowe,
- pokonanie zabezpieczeń fizycznych lub programowych,

- ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe,
- udostępnianie danych osobowych osobom nieupoważnionym,
- niedyskrecja osób upoważnionych do przetwarzania danych osobowych,
- podsłuch lub podgląd danych osobowych,
- niekontrolowana obecność osób nieupoważnionych w obszarze przetwarzania danych osobowych,
- nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik,
- utrata nośnika zawierającego dane osobowe,
- nieuprawnione wyniesienie danych osobowych zawartych na nośniku,
- naprawy i konserwacje systemów lub sieci teleinformatycznej służących do przetwarzania danych osobowych przez osoby nieupoważnione do przetwarzania danych osobowych,
- elektromagnetyczna emisja ujawniająca,
- stosowanie korupcji oraz szantażu w celu wydobycia określonych informacji od wybranych pracowników biblioteki.

Skala identyfikacji skutków utraty zasobów dla atrybutu poufności danych osobowych.	
Wartość	Skutki
< 0 >	Brak skutków utraty poufności
< 1 – 3 >	Niski skutek utraty poufności
< 4 – 7 >	Średni skutek utraty poufności
< 8 – 9 >	Wysoki skutek utraty poufności
< 9 – 10 >	Całkowita utrata poufności

Integralność

Integralność, to cecha zapewniająca, że dane nie zostały zmodyfikowane lub zniszczone w sposób nieautoryzowany.

Zagrożenia, jakie można wyróżnić ze względu na utratę integralności przez system:

- nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego,
- błędy, pomyłki,
- brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez Administratora lub użytkownika,
- wadliwe działanie systemu operacyjnego,
- brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych,
- celowe lub przypadkowe uszkodzenie systemu operacyjnego lub urządzeń sieciowych,
- celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych,
- działanie złośliwego oprogramowania (wirusy),
- pożar, zalanie, ekstremalna temperatura, itp.,

- zagrożenia zewnętrzne (np. klęski żywiołowe, atak terrorystyczny).

Skala identyfikacji skutków utraty zasobów dla atrybutu integralności danych osobowych.	
Wartość	Skutki
< 0 >	Utrata integralności nie występuje
< 1 – 3 >	Niski skutek utraty integralności
< 4 – 7 >	Średni skutek utraty integralności
< 8 – 9 >	Wysoki skutek utraty integralności
< 10 >	Bezwzględny skutek utraty integralności

Rozliczalność

Rozliczalność to cecha zapewniająca działanie podmiotu przetwarzającego dane osobowe, która może być przypisana w sposób jednoznaczny tylko temu jednemu podmiotowi.

Zagrożenia, jakie można wyróżnić ze względu na utratę rozliczalności systemu:

- brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania,
- wprowadzenie zmian w treści dokumentu zawierającego dane osobowe,
- błędy oprogramowania lub sprzętu,
- nieprzydzielenie użytkownikom indywidualnych identyfikatorów,
- niewłaściwa administracja systemem informatycznym,
- niewłaściwa konfiguracja systemu informatycznego,
- zniszczenie lub sfałszowanie logów systemowych,
- brak rejestracji udostępnienia danych osobowych,
- podszywanie się pod innego użytkownika,
- niespełnienie przez system wymagań ustanowionych w dokumentacji wewnętrznej ochrony danych osobowych.

Skala identyfikacji skutków utraty zasobów dla atrybutu rozliczalności danych osobowych.	
Wartość	Skutki
< 0 >	Utrata rozliczalności nie występuje
< 1 – 3 >	Niski skutek utraty rozliczalności
< 4 – 6 >	Średni skutek utraty rozliczalności
< 7 – 8 >	Wysoki skutek utraty rozliczalności

< 9 >	Ekstremalny skutek utraty rozliczalności

Podatność systemu ochrony danych osobowych na zagrożenia

Podatność systemu to słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie.

Przebieg kontroli podatności systemu ochrony danych osobowych		
Lp.	Zakres kontroli	Podejmowane czynności
1	Dokumentacja	Sprawdzenie, czy dokumentacja ODO jest aktualna względem obowiązującego stanu prawnego oraz faktycznego.
2	Dokumentacja	Sprawdzenie, czy osoby, które mają dostęp do danych osobowych, mają upoważnienia do przetwarzania danych osobowych - upoważnienie powinno odzwierciedlać zakres obowiązków.
3	Dokumentacja	Sprawdzenie, czy osoby, które mogą mieć dostęp do danych osobowych, ale nie są upoważnione, podpisały oświadczenie o zachowaniu poufności.
4	Dokumentacja	Sprawdzenie, czy prowadzona jest aktualna ewidencja osób przetwarzających dane osobowe.
5	Fizyczna ochrona danych osobowych	Kontrolowanie osób przetwarzających dane osobowe - czy stosują się do „zasady czystego biurka”.
6	Fizyczna ochrona danych osobowych	Sprawdzenie, czy w pomieszczeniu znajdują się szafy zamykane na klucz, w których przechowuje się dokumentację zawierającą dane osobowe podlegające ochronie.
7	Fizyczna ochrona danych osobowych	Sprawdzenie, czy w pomieszczeniu znajduje się niszczarka dokumentów (jeśli nie to w jaki sposób niszczy się zbędną dokumentację, która nie podlega archiwizacji).
8	Ochrona środowiska komputerowego	Kontrola sposobu uwierzytelnienia użytkowników systemu (systemów) informatycznego.
9	Ochrona środowiska komputerowego	Kontrolowanie aktywności systemu antywirusowego.
10	Ochrona środowiska komputerowego	Kontrolowanie, czy pracownik korzysta z wygaszacza ekranu.
11	Ochrona środowiska komputerowego	Sprawdzenie, czy monitor komputera został usytuowany w sposób uniemożliwiający wgląd do danych - osobom postronnym.

12	Kontrola praktyki	Przeprowadzenie sprawdzenia pod kątem : • próby nieuprawnionego dostępu do danych osobowych, • działanie zewnętrznych aplikacji, wirusów czy złośliwego oprogramowania, • nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym, • próba nieuprawnionej interwencji przy sprzęcie komputerowym, • wynoszenie niezabezpieczonych pamięci z miejsca pracy, • udzielanie informacji osobom postronnym, pomijając formalny tryb administracyjny.

Skala identyfikacji podatności systemu na określone zagrożenia.	
Wartość	Skutki
< 0 >	Brak podatności
< 1 – 4 >	Niski poziom
< 5 – 7 >	Średni poziom
< 8 – 9 >	Wysoki poziom
< 10 >	Ekstremalny poziom

Analiza zagrożeń i szacowanie ryzyka

Aby poprawnie przeprowadzić analizę ryzyka, Administrator Danych Osobowych określa:

1. Zasoby, które będzie chronić:
   - sprzęt komputerowy przechowujący dane (dysk twardy),
   - dane osobowe przetwarzane w formie papierowej i elektronicznej,
   - aplikacje, w których przetwarzane są dane osobowe,
   - pomieszczenia, w których pracują osoby przetwarzające dane osobowe.
2. Zagrożenia - czynnik, który może powodować wystąpienie incydentu naruszenia.
3. Podatność - słabość zasobów, która może być wykorzystana przez potencjalne zagrożenie.
4. Skutki - jaki wpływ będzie miał zaistniały incydent na utratę danych osobowych.
5. Ryzyko - iloczyn wartości skutków i prawdopodobieństwa wystąpienia zagrożenia.

Określenie poziomu ryzyka utraty bezpieczeństwa danych osobowych:

- niski - niskie szkody w przypadku realizacji zagrożenia i niska możliwość jego wystąpienia,
- średni - wysokie szkody w przypadku realizacji zagrożenia i niska możliwość jego realizacji bądź niskie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego realizacji,

- wysoki - wysokie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego wystąpienia,
- maksymalny - wysokie szkody w przypadku realizacji zagrożenia oraz wysoka możliwość jego wystąpienia, skutkująca nie tylko na organizację, ale na podmioty trzecie.

Skala identyfikacji poziomu ryzyka	
Wartość	Poziom ryzyka
<1-20>	Niski poziom ryzyka utraty bezpieczeństwa danych osobowych
<21-60>	Średni poziom ryzyka utraty bezpieczeństwa danych osobowych
<61-80>	Wysoki poziom ryzyka utraty bezpieczeństwa danych osobowych
<81-100>	Maksymalny poziom ryzyka utraty bezpieczeństwa danych osobowych

Administrator Danych Osobowych wyznacza poziom ryzyka akceptowalnego, powyżej którego będą określone działania zapobiegawcze i/lub korygujące. W przypadku, kiedy wartość oszacowanego ryzyka przekracza próg ryzyka akceptowalnego, ADO podejmuje działania wdrażające stosowne zabezpieczenia. Tabelę szacowania ryzyka oraz wnioski i działania naprawcze ADO stanowi **Załącznik nr 1**.

Administrator Danych Osobowych po oszacowaniu ryzyka przystępuje do etapu postępowania z ryzykiem, w ramach którego może podjąć cztery różne działania:

- unikanie ryzyka - odejście od działań, które wiążą się z ryzykiem, jeżeli ryzyko jest duże, a system, w którym ono występuje, nie przynosi odpowiednich korzyści,
- ograniczenie ryzyka (redukcja) - podjęcie działań ograniczających ryzyko lub zmniejszających podatność,
- przekazanie ryzyka - przeniesienie ryzyka na podmiot zewnętrzny, odpowiedzialność zostaje przekazana w odpowiednich zapisach umowy,
- akceptacja ryzyka - gdy koszty działań w celu niwelowania ryzyka przekraczają oczekiwane lub występują określone trudności w przeciwdziałaniu ryzyka.

Załączniki

Załącznik nr 1	- Tabela szacowania ryzyka oraz wnioski i działania naprawcze ADO.