Załącznik do zarządzenia nr 17/10/2020
Dyrektora Biblioteki Publicznej im. Jana Pawła II w Dzielnicy Rembertów m.st. Warszawy
z dnia 23.10.2020 r.

Polityka bezpieczeństwa danych osobowych

Biblioteki Publicznej im. Jana Pawła II w Dzielnicy Rembertów m.st. Warszawy

Spis treści

Wstęp

Polityka Bezpieczeństwa Danych Osobowych (dalej: „PBDO") określa politykę oraz zasady zarządzania ochroną zbiorów danych osobowych w Bibliotece Publicznej im. Jana Pawła II w Dzielnicy Rembertów m.st. Warszawy (dalej: Biblioteka), podlegających ochronie prawnej. Dokument zawiera wymagania bezpieczeństwa oraz zalecenia szczegółowe, wynikające bezpośrednio z Ustawy o ochronie danych osobowych i aktów wykonawczych. Obowiązek posiadania Polityki Bezpieczeństwa, a także opis jej „konstrukcji" są przewidziane w następujących przepisach:

1. Rozporządzenie Parlamentu Europejskiego w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,
2. Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018r. poz. 1000)
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004 nr 100 poz. 1024),
4. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. 2015 poz. 719)
5. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. 2015 poz. 745)
6. Rozporządzenie 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. 2012 poz. 526).

Celem niniejszego dokumentu jest określenie:

- podstaw do wdrożenia i rozwoju Systemu Ochrony Danych Osobowych,
- zasad przetwarzania danych osobowych zgodnych z przepisami prawa,
- ochrony danych osobowych przed udostepnieniem osobom nieupoważnionym, przetwarzaniem przez osoby nieuprawnione w tym zmianą, uszkodzeniem lub zniszczeniem,
- obowiązków osób odpowiedzialnych za przetwarzanie danych osobowych jak i osób odpowiedzialnych za ich bezpieczeństwo.

PBDO stanowi zbiór zasad, które obowiązują w stosunku do zidentyfikowanych zbiorów danych osobowych, niezależnie od formy przetwarzania, których administratorem danych w myśl Rozporządzenia Parlamentu Europejskiego w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, jest Biblioteka Publiczna im. Jana Pawła II w Dzielnicy Rembertów m.st. Warszawy. Ustanowione w niniejszej polityce zasady muszą być stosowane przez wszystkie osoby posiadające dostęp do danych osobowych.

Niniejszy dokument dotyczy wszystkich osób zatrudnionych, współpracujących lub świadczących usługi na rzecz Biblioteki, a także innych osób, mających dostęp do informacji, stanowiących dane osobowe. Wszyscy pracownicy oraz inne osoby upoważnione do przetwarzania danych osobowych w Bibliotece mają obowiązek zapoznania się z niniejszym dokumentem i postępowania zgodnie z jego postanowieniami oraz innymi

dokumentami wchodzącymi w skład dokumentacji systemu ochrony danych osobowych, w zakresie, w jakim te instrukcje i dokumenty zostały im udostępnione.

1. Podstawowe definicje

1. **Administrator Danych Osobowych (ADO) –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem danych jest ten, kto decyduje o celach i środkach przetwarzania danych, czyli Biblioteka im. Jana Pawła II w Dzielnicy Rembertów m.st. Warszawy, którą reprezentuje dyrektor.
2. **Inspektor Ochrony Danych Osobowych (IODO)** – osoba wyznaczona przez administratora danych osobowych, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych,
3. **RODO** – rozporządzenie 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.L nr 119, **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
4. **Zbiór danych osobowych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie,
5. **Przetwarzane danych –** operacja lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, łączenie, przesyłanie, zmienianie, udostępnianie i usuwanie, niszczenie, itd., a zwłaszcza te, które wykonuje się w systemach informatycznych,
6. **System informatyczny (SI) –** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,
7. **Administrator Systemu Informatycznego (ASI)** – osoba lub osoby, upoważnione przez administratora danych osobowych do administrowania systemami informatycznymi,
8. **Kontrahent –** osoba fizyczna lub prawna, jednostka organizacyjna nie posiadająca osobowości prawnej lub inny podmiot niż osoba, której dane dotyczą, które z upoważnienia administratora danych osobowych mogą przetwarzać dane osobowe.
9. **Użytkownik** – osoba mająca upoważnienie do przetwarzania danych osobowych w Bibliotece.

1.2. Skróty

1. **PBDO** – Polityka Bezpieczeństwa Danych Osobowych
2. **IODO** – Inspektor Ochrony Danych Osobowych
3. **ADO** – Administrator Danych Osobowych
4. **ASI** – Administrator Systemu Informatycznego
5. **IZSI** – Instrukcja Zarządzania Systemami Informatycznymi Mateusz, CafeSuite, Finka-FK, Finka-Płace, Płatnik oraz pakietami aplikacji biurowych
6. **SI** – System Informatyczny
7. **RODO** – Rozporządzenie Parlamentu Europejskiego w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

2. Postanowienia ogólne

Celem Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Bibliotece jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe (zarówno metodami tradycyjnymi i w systemach informatycznych), jak również ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osoby nieuprawione, zmianą, uszkodzeniem lub zniszczeniem. PBDO określa również zakres obowiązków osób odpowiedzialnych za przetwarzanie danych osobowych, jak i osób odpowiedzialnych za ich bezpieczeństwo.

2.1. Cel Polityki

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników, proporcjonalnie i adekwatnie do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach prowadzonej działalności. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Bibliotece rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest akceptowalna wielkość ryzyka związanego z ochroną danych osobowych. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

- poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
- integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
- integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej,
- dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
- zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

Postanowienia dotyczące przetwarzania danych osobowych są elementem organizacji i porządku pracy w Bibliotece.

2.2. Zakres ochrony danych osobowych

W Bibliotece przetwarzane są zbiory danych, w stosunku do których Biblioteka posiada status administratora danych. Przetwarzane są dane osobowe czytelników, użytkowników Internetu, uczestników wydarzeń bibliotecznych, pracowników, kandydatów do pracy, osób współpracujących, kontrahentów zebrane w zbiorach danych osobowych. Informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej. Polityka bezpieczeństwa zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych. Szczegółowy wykaz zbiorów danych, zawierający charakterystykę tych zbiorów oraz opis przepływów danych pomiędzy systemami informatycznymi służącymi do przetwarzania tych zbiorów znajdują się w *Załączniku nr 1: Wykaz zbiorów danych osobowych wraz ze wskazaniem programów i metod zastosowanych do przetwarzania danych osobowych* do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

Politykę bezpieczeństwa stosuje się w szczególności do:

- danych osobowych przetwarzanych w systemie: Mateusz, CafeSuite, Finka-FK, Finka-Płace, Płatnik oraz pakietami aplikacji biurowych,

- wszystkich informacji dotyczących danych osobowych czytelników, użytkowników, pracowników, kontrahentów i innych osób współpracujących z Biblioteką,
- odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia,
- informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
- rejestru pracowników i osób współpracujących mających upoważnienia administratora danych osobowych do przetwarzania danych osobowych,
- innych dokumentów zawierających dane osobowe.

Zakresy ochrony danych osobowych określone przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty mają zastosowanie do:

- wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych, w których przetwarzane są dane osobowe podlegające ochronie, oraz zbiorów danych na nośnikach papierowych,
- wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane dane podlegające ochronie,
- wszystkich pracowników, osób współpracujących i innych osób mających dostęp do danych podlegających ochronie.

3. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów i metod zastosowanych do przetwarzania danych osobowych.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów i metod zastosowanych do przetwarzania tych danych zamieszczony jest w *Załączniku nr 1: Wykaz zbiorów danych osobowych wraz ze wskazaniem programów i metod zastosowanych do przetwarzania danych osobowych* do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

4. Organizacja wewnętrzna w zakresie ochrony danych osobowych - role i odpowiedzialności w zakresie ochrony danych osobowych.

W celu efektywnego zarządzania ochroną danych osobowych w Bibliotece funkcjonuje formalna organizacja wewnętrzna, w skład której wchodzą następujące role: Administrator Danych Osobowych (ADO), Inspektor Ochrony Danych Osobowych (IODO), Administrator Systemu Informatycznego (ASI) oraz Użytkownik.

4.1. Administrator Danych Osobowych (ADO)

1. ADO jest Biblioteka, osoba pełniąca obowiązki ADO - dyrektor Biblioteki. ADO pełni funkcje na zasadach i w zakresie określonym w RODO. ADO:
    a. definiuje i zatwierdza PBDO oraz IZSI,
    b. nadzoruje realizacje postanowień PBDO oraz IZSI,
    c. określa sposób, w jaki dane osobowe są zarządzane, zabezpieczane i przetwarzane,
    d. zapewnia niezbędne zasoby potrzebne do odpowiedniego funkcjonowania PBDO oraz IZSI,
    e. wyznacza osobę do realizacji obowiązków IODO,
    f. wyznacza osobę do realizacji obowiązków ASI
    g. zatwierdza kierunki rozwoju i doskonalenia PBDO proponowane przez IODO,
    h. ewidencjonuje zbiory danych osobowych zgodnie z przyjętymi zasadami wraz z opisem struktury zbiorów wskazującym zawartość poszczególnych pól informacyjnych oraz wskazaniem aplikacji służących do ich przetwarzania,

i. wykonuje obowiązki wyznaczania i przestrzegania zasad ochrony danych osobowych pod kątem zabezpieczeń teleinformatycznych określonych w pkt 4.3, chyba że został powołany ASI

2. ADO odpowiada za zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
   a. sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
   b. nadzorowanie opracowania i aktualizowania dokumentacji, opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
   c. nadzorowanie przestrzegania zasad określonych w dokumentacji, o której mowa w ppkt. b,
   d. zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
3. ADO dokonuje inne czynności z zakresu ochrony danych osobowych, w tym:
   a. nadzoruje i monitoruje przestrzeganie zasad ochrony przetwarzanych informacji w Bibliotece.
   b. wydaje upoważnienia do przetwarzania danych osobowych;
   c. prowadzi rejestr użytkowników upoważnionych do przetwarzania danych osobowych (*Rejestr upoważnień*);
   d. realizuje proces spełnienia żądań osób, których dane osobowe dotyczą;
   e. zarządza incydentami bezpieczeństwa danych osobowych – realizuje procedurę obsługi incydentów, analizuje incydenty, wszczyna postępowanie wyjaśniające w związku z incydentami oraz prowadzi *Rejestr naruszeń* (patrz: *Załącznik nr 11* do niniejszej Polityki Bezpieczeństwa Danych Osobowych);
   f. prowadzi *Rejestr czynności przetwarzania danych osobowych* (patrz: *Załącznik nr 4* do niniejszej Polityki Bezpieczeństwa Danych Osobowych;
   g. odpowiada za identyfikowanie i zarządzanie zbiorami danych osobowych;
   h. określa narzędzia, metody, miejsce i czas przetwarzania informacji w zbiorach danych;
   i. wyraża zgodę na udostępnianie informacji zgodnie z przepisami prawa.
   j. realizuje wszystkie inne zadania wymienione w Polityce Bezpieczeństwa Danych Osobowych nieprzypisane do obowiązków innych osób.
4. ADO jest odpowiedzialny za okresową realizację szacowania ryzyka utraty bezpieczeństwa danych osobowych.
5. ADO określa narzędzia, metody, miejsce i czas przetwarzania informacji w zbiorach danych.

4.2. Inspektor Ochrony Danych Osobowych (IODO)

1. IODO może być osoba, która:
   a. ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych,
   b. posiada odpowiednią wiedzę w zakresie ochrony danych osobowych,
   c. nie była karana za umyślne przestępstwo.
2. IODO ma następujące zadania:
   a. informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów o ochronie danych osobowych i doradzanie im w tej sprawie;
   b. informowanie administratora o konieczności dostosowania wewnętrznych regulacji dotyczących danych osobowych do zmian przepisów prawa;
   c. monitorowanie przestrzegania RODO, innych przepisów o ochronie danych osobowych, w tym działania zwiększające świadomość, m.in. szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   d. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania; współpraca z organem nadzorczym; pełnienie funkcji punktu kontaktowego dla

organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, zapoznawanie pracowników z regulacjami dotyczącymi bezpieczeństwa danych osobowych.

3. IODO corocznie przygotowuje plan sprawdzeń, przeprowadza je oraz przygotowuje sprawozdania z funkcjonowania systemu danych osobowych.

4.3. Administrator Systemu Informatycznego (ASI)

1. Podstawowym zadaniem ASI jest wyznaczania i wdrażanie zasad ochrony danych osobowych pod kątem zabezpieczeń teleinformatycznych, w tym m.in.:
    a. przygotowanie i wdrażanie dokumentacji ochrony danych osobowych, w szczególności instrukcji zarządzania systemem informatycznym,
    b. współpraca przy przeprowadzaniu okresowych planów sprawdzeń, czyli systematyczne kontrolowanie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności kontrola pod kątem zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym,
    c. zapewnienia ciągłości działania systemu, w tym zabezpieczenie zbiorów poprzez systematyczne wykonywanie kopii zapasowych,
    d. nadzór nad naprawą oraz likwidacją urządzeń komputerowych w tym nośników danych osobowych,
    e. realizowanie ustalonych zabezpieczeń systemów służących do przetwarzania danych osobowych przed działaniem oprogramowania złośliwego, którego celem może okazać się uzyskanie nieuprawnionego dostępu do danych.

4.4. Użytkownik

Obowiązkiem użytkownika jest :

a. przestrzeganie postanowień oraz zasad ustanowionych przez PBDO oraz IZSI w adekwatnym zakresie,
b. zabezpieczenie przekazanych do przetwarzania danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem,
c. niezwłoczne informowanie bezpośredniego przełożonego oraz ADO w przypadku zidentyfikowania wszelkich naruszeń w zakresie bezpieczeństwa danych osobowych.

5. Wymagania dotyczące zabezpieczenia danych osobowych

5.1. Organizacyjne środki ochrony

5.1.1. Zasady dopuszczania do przetwarzania danych osobowych

Szkolenie i zobowiązanie do zachowania tajemnicy

1. Wszyscy pracownicy zatrudnieni przy przetwarzaniu danych osobowych muszą zostać zapoznani z obowiązującymi w Bibliotece przepisami dotyczącymi ochrony danych osobowych oraz podpisać zobowiązanie do zachowania w tajemnicy danych osobowych, do których będą mieli dostęp przed przystąpieniem do pracy z danymi osobowymi.
2. Pracownikom zatrudnionym na podstawie umowy, ADO przekazuje do zapoznania się materiały o obowiązujących w Bibliotece przepisach, dotyczących ochrony danych osobowych. Następnie odbiera od pracownika zobowiązanie do zachowania w tajemnicy danych osobowych, do których przetwarzania zostanie dopuszczony, zgodnie z *Załącznikiem nr 2: Wzór zobowiązania do zachowania w poufności danych osobowych* do niniejszej Polityki Bezpieczeństwa Danych Osobowych. Zobowiązanie to przechowuje się w aktach osobowych pracownika.

3. Kontrahentów Biblioteki z przepisami dotyczącymi ochrony danych osobowych w Bibliotece zapoznaje osoba odpowiedzialna za współpracę (tzw. opiekun).

Zarządzanie upoważnieniami do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych mogą być dopuszczone tylko osoby posiadające ważne upoważnienie do przetwarzania danych osobowych w zbiorze danych osobowych Biblioteki oraz w zbiorach danych osobowych powierzonych w ramach zawartych umów.
2. Upoważnienia do przetwarzania danych osobowych w Bibliotece wystawia i zatwierdza ADO na podstawie:
    a. zobowiązania do zachowania w tajemnicy danych osobowych,
    b. informacji na temat miejsca zatrudnienia (komórki organizacyjnej) osoby w Bibliotece.
3. ADO prowadzi i aktualizuje w formie elektronicznej lub papierowej *Rejestr upoważnień*.
4. *Rejestr upoważnień* zawiera co najmniej:
    a. numer upoważnienia,
    b. imię i nazwisko osoby upoważnionej,
    c. nazwę zbioru danych osobowych oraz zakres upoważnienia,
    d. identyfikator oraz nazwa systemu informatycznego,
    e. datę nadania upoważnienia,
    f. datę odebrania upoważnienia.
5. ADO jest obowiązany do przekazywania informacji o wydanych i odwołanych upoważnieniach poszczególnym pracownikom oraz ich przełożonym.
6. ADO obowiązany jest do udostępnienia do wglądu IODO *Rejestru upoważnień*.

Wydawanie upoważnień

1. Upoważnienia są wydawane pracownikom lub przedstawicielom firm zewnętrznych, którym jest to niezbędne w celu właściwego wykonywania obowiązków służbowych.
2. Wniosek o wydanie upoważnienia dla osoby zatrudnionej w danej komórce organizacyjnej, która będzie przetwarzała dane osobowe w zbiorze, zgłasza do ADO osoba kierująca komórką. Upoważnienie może zostać wydane pracownikowi, który spełnił wymagania określone w punkcie *Szkolenie i zobowiązanie do zachowania tajemnicy* na wzorze, który przedstawia *Załącznik nr 3: Wzór upoważnienia do przetwarzania danych osobowych* do niniejszej Polityki Bezpieczeństwa Danych Osobowych.
3. Oryginał upoważnienia wydawany jest upoważnionemu pracownikowi, kopie upoważnień przechowuje ADO.

Wygaśnięcie upoważnień

1. Upoważnienie wygasa w przypadku:
    a. upływu okresu jego ważności,
    b. odwołania,
    c. ustania stosunku pracy bądź rozwiązania innej umowy.
2. O odwołanie upoważnienia oraz o cofnięcie uprawnień w SI może wystąpić do ADO bezpośredni przełożony pracownika, którego upoważnienie dotyczy.
3. ADO dokonuje odpowiednich zmian w *Rejestrze upoważnień*, wpisując datę ustania upoważnienia oraz niezwłocznie informuje ASI oraz pracownika, którego upoważnienie dotyczy, o jego odwołaniu.

5.1.2. Zarządzanie rejestrem zbiorów danych osobowych

Potrzeba przetwarzania nowego zbioru danych osobowych

1. W Bibliotece zabronione jest przetwarzanie danych osobowych w zbiorze danych osobowych, jeśli zbiór taki nie figuruje w *Rejestrze czynności przetwarzania*, którego wzór stanowi *Załącznik nr 4: Rejestr czynności przetwarzania danych osobowych* do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

2. Pracownik zgłasza potrzebę utworzenia nowego zbioru danych osobowych ADO oraz przekazują wszystkie stosowne informacje dotyczące nowego zbioru. Utworzenie nowego zbioru danych osobowych może być wynikiem:
    a. realizacji określonego celu,
    b. przyjęcia zbioru danych osobowych w wyniku zawarcia umowy o powierzeniu przetwarzania lub przekazania zbioru danych osobowych należących do innego podmiotu.

Tworzenie zbioru danych

1. ADO, po otrzymaniu zgłoszenia dotyczącego potrzeby utworzenia nowego zbioru danych osobowych, analizuje zawartość informacyjną zgłaszanego zbioru oraz określa, czy zbiór jest nowym zbiorem danych osobowych na podstawie:
    a. zakresu danych (pól informacyjnych),
    b. celu przetwarzania danych zawartych w zbiorze.
2. ADO:
    a. informacje o zbiorze wpisuje do *Rejestru czynności przetwarzania danych osobowych* (patrz: *Załącznik nr 4* do niniejszej Polityki Bezpieczeństwa Danych Osobowych) oraz przygotowuje *Księgę rejestrową* dla każdego zarejestrowanego zbioru, której wzór zawiera *Załącznik nr 5: Wzór Księgi Rejestrowej* do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

Aktualizacja zgłoszenia zbioru danych osobowych

1. Aktualizacji zgłoszenia zbioru danych osobowych w *Rejestrze czynności przetwarzania danych osobowych* wymagają w szczególności następujące sytuacje:
    a. zamiar powierzenia przetwarzania danych osobowych administrowanych przez Bibliotekę innemu podmiotowi w wyniku podpisania umowy,
    b. zamiar przekazania danych osobowych administrowanych przez Bibliotekę innemu podmiotowi w wyniku podpisania umowy,
    c. dokonanie zmian w warunkach technicznych, organizacyjnych lub prawnych związanych ze zgłoszonym zbiorem danych osobowych, wpływających na zmianę treści zgłoszenia.
2. ADO podejmuje decyzję o konieczności aktualizacji informacji o zbiorze w *Rejestrze czynności przetwarzania danych osobowych* wraz z odpowiednimi *Księgami rejestrowymi*.

Usuwanie zbioru danych osobowych

1. Decyzję o usunięciu każdego zbioru danych osobowych podejmuje ADO.
2. Wykreślenie zbioru danych osobowych z *Rejestru czynności przetwarzania danych osobowych następuje* niezwłocznie po zaprzestaniu przetwarzania danych w zbiorze.
3. Wykreślenie zbioru danych osobowych z *Rejestru...* dokonuje się poprzez założenie kolejnej wersji księgi rejestrowej, w której zamieszcza się odpowiednią wzmiankę.
4. ADO jest zobowiązany do podjęcia działań mających na celu wyrejestrowanie zbioru danych z *Rejestru czynności przetwarzania danych osobowych*, poprzez zainicjowanie procesu komisyjnego fizycznego usunięcia danych osobowych (w formie papierowej oraz elektronicznej) z uwzględnieniem wymogów procedur wewnętrznych oraz przepisów o archiwizacji danych.

Odnotowywanie zmian w *Rejestrze czynności przetwarzania danych osobowych*

1. ADO tworzy historię zmian w *Rejestrze...* i odnotowuje informacje o wszelkich dokonywanych w nim zmianach.

5.1.3. Inwentaryzacja zasobów wspierających przetwarzanie danych osobowych

1. ADO odpowiedzialny jest za inwentaryzację zasobów wspierających przetwarzanie informacji zgodnie z *Załącznikiem nr 6: Inwentaryzacja zasobów wspierających przetwarzanie danych osobowych* do niniejszej Polityki Bezpieczeństwa Danych Osobowych.
2. Inwentaryzacja podlega okresowej aktualizacji (przynajmniej raz do roku).
3. Inwentaryzacja zasobów stanowi informację wejściową do procesu szacowania ryzyka utraty bezpieczeństwa danych osobowych.

5.1.4. Szacowanie ryzyka utraty bezpieczeństwa danych osobowych

1. ADO odpowiedzialny jest za okresową realizację szacowania ryzyka utraty bezpieczeństwa danych osobowych.
2. Aktualizacja wyników szacowania ryzyka realizowana jest przynajmniej raz do roku.
3. Wyniki szacowania ryzyka oraz planowane działania minimalizujące ryzyko zatwierdzane są przez ADO.

5.1.5. Spełnienie obowiązku informacyjnego

1. W stosunku do osób, których dane osobowe Biblioteka zbiera w celu włączenia ich do zbiorów i dalszego przetwarzania należy spełnić obowiązek informacyjny.
2. Obowiązek informacyjny należy spełnić w przypadku:
    a. zbierania danych osobowych od osoby, której one dotyczą (art. 13 RODO) w momencie pozyskiwania danych,
    b. zbierania danych osobowych nie od osoby, której one dotyczą (art. 14 RODO) bezpośrednio po utrwaleniu danych osobowych.
3. Spełnienie obowiązku informacyjnego nie jest konieczne, jeżeli:
    a. osoba, której dane dotyczą, dysponuje już tymi informacjami, co Biblioteka jest w stanie wykazać,
    b. pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem polskim, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą.
4. Wykaz wzorów oświadczeń o spełnieniu obowiązku informacyjnego stanowi *Załącznik nr 7: Klauzula informacyjna administratora o przetwarzaniu danych osobowych* do niniejszej Polityki Bezpieczeństwa Danych Osobowych.
5. Za należyte spełnienie obowiązku informacyjnego w stosunku do osób fizycznych, których dane są przetwarzane przez Bibliotekę odpowiada ADO.

5.1.6. Realizacja praw osoby, której dane osobowe dotyczą

1. Spełnienie praw osoby, której dane dotyczą obejmuje:
    a. prawo do sprostowania danych (art. 16 RODO),
    b. prawo do usunięcia danych (art. 17 RODO), z wyjątkiem gdy przetwarzanie jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa polskiego, lub do wykonania zadania realizowanego w interesie publicznym, lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
    c. prawo do ograniczenia przetwarzania (art. 18 RODO),
    d. prawo do przenoszenia danych (art. 20 RODO),
    e. prawo do sprzeciwu w przypadkach związanych ze szczególną sytuacją osoby, które dane dotyczą, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 21 RODO).
2. Spełnienie praw osoby wymaga złożenia do ADO pisemnego wniosku, precyzującego żądanie Wnioskodawcy.
3. W przypadku pozytywnego rozpatrzenia wniosku, ADO ustala sposób realizacji żądań. W szczególności:
    a. ASI pod nadzorem ADO realizuje czynności mające na celu wstrzymanie przetwarzania danych osobowych w SI,

b. ADO realizuje czynności mające na celu wstrzymanie przetwarzania danych osobowych w formie papierowej.

4. ADO obowiązany jest rozpatrzyć i zrealizować wniosek w terminie do 30 dni od momentu wpłynięcia wniosku do Biblioteki.

5.1.7. Powierzenie przetwarzania danych osobowych

1. W uzasadnionych przypadkach wynikających z realizacji zadań, dopuszcza się powierzenie przetwarzania danych osobowych podmiotowi zewnętrznemu.
2. Treść umowy dotyczącej powierzenia przetwarzania danych osobowych musi obejmować elementy określone w art. 28 ust. 3 RODO, w tym co najmniej:
   a. zakres i cel przetwarzania danych osobowych,
   b. zobowiązanie podmiotu, któremu powierza się dane, do zastosowania środków zabezpieczających dane osobowe oraz zapewnienie podmiotu przetwarzającego, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania ich w tajemnicy,
   c. oświadczenie o podjęciu środków wymaganych na mocy art. 32 RODO,
   d. określenie sposobu sprawowania przez Bibliotekę kontroli należytego wykonania umowy w powyższym zakresie,
   e. określenie sposobu dochodzenia roszczeń Biblioteki w przypadku, gdy nastąpi naruszenie ochrony danych z przyczyn leżących po stronie podmiotu, któremu przetwarzanie danych powierzono,
   f. określenie odpowiednich środków technicznych i organizacyjnych w celu wywiązania się z obowiązku odpowiadania na żądania osoby, której dane dotyczą w zakresie wykonywania jej praw określonych w rozdziale III RODO, określenie zasad informowania współpracy przy realizacji obowiązków określonych w art. 32–36 RODO,
   g. określa zasady postępowania z informacjami po zakończeniu świadczenia usług związanych z przetwarzaniem danych,
   h. umożliwienie administratorowi lub upoważnionemu audytorowi przeprowadzenie audytu u podmiotu przetwarzającego.
4. Każdorazowo umowę podpisuje ADO.
5. ADO jest obowiązany do aktualizacji informacji o zawartej umowie w *Rejestrze czynności przetwarzania danych osobowych* (patrz: *Załącznik nr 4* do niniejszej Polityki Bezpieczeństwa Danych Osobowych).

5.1.8. Udostępnianie danych osobowych

1. Wszystkie dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis prawa stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
2. Wszystkie wnioski o udostępnienie danych osobowych przekazywane są do ADO.
3. ADO rozpatruje wniosek o udostępnienie danych osobowych pod kątem spełnienia wymagań formalnych. W szczególności sprawdza czy wniosek zawiera:
   a. dane o wnioskodawcy,
   b. zakres żądanych informacji,
   c. cel pozyskania danych,
   d. podstawę prawną upoważniającą do pozyskania informacji.
4. Jeśli wniosek nie zawiera któregoś z powyżej wskazanych elementów, wnioskodawcę wzywa się do o uzupełnienia wniosku.
5. ADO podejmuje decyzję dotyczącą udostępnienia danych osobowych.
6. Jeśli wniosek spełnia wymagania, o których mowa w pkt. 3, ADO:
   a. przygotowuje pismo do wnioskodawcy informujące o negatywnym rozpatrzeniu wniosku o udostępnienie danych osobowych bądź

b. przygotowuje żądane dane i wysyła odpowiedź do wnioskodawcy oraz odnotowuje udostępnienie we właściwych rejestrach udostępnień, które prowadzone są w formie papierowej.

7. Informacje zawierające dane osobowe są przekazywane uprawnionym podmiotom:
   a. listem poleconym za potwierdzeniem odbioru,
   b. w drodze teletransmisji danych, zgodnie z procedurami ochrony danych podczas transmisji,
   c. osobiście za potwierdzeniem odbioru,
   d. w inny sposób określony przepisami prawa lub umową.

5.1.9. Uwzględnianie ochrony danych w fazie projektowania

1. W przypadku określania nowych sposobów przetwarzania danych osobowych (np. tworząc nowy zbiór danych osobowych, wdrażając nowy system informatyczny) lub modyfikacji dotychczas stosowanych sposobów i środków przetwarzania danych osobowych ADO obowiązany jest zaprojektować i wdrożyć odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych.
2. W celu identyfikacji odpowiednich zabezpieczeń należy przeprowadzić szacowanie ryzyka zgodnie z zasadami określonymi w *Załączniku nr 8: Szacowanie ryzyka utraty bezpieczeństwa danych osobowych* do niniejszej Polityki Bezpieczeństwa Danych Osobowych.
3. Przy zakupie gotowych rozwiązań informatycznych ADO powinien wybierać te, które posiadają zaimplementowane zabezpieczenia służące zabezpieczeniu danych.

5.1.10. Aktualizacja dokumentacji

1. ADO na bieżąco monitoruje zaplanowane procesy przetwarzania danych osobowych w celu stwierdzenia konieczności opracowania dokumentacji w tym zakresie.
2. Propozycje zmian do aktualnie obowiązującej dokumentacji, propozycje nowych zapisów lub konkretnych dokumentów zgłasza IODO.
3. ADO na bieżąco monitoruje aktualność dokumentacji. Aktualizacja powinna być wykonana w terminie 21 dni od dnia wystąpienia zmiany stanu faktycznego w procesie przetwarzania danych osobowych.
4. ADO zatwierdza dokumentacje w sposób przyjęty w Bibliotece oraz wdraża ją do stosowania.

5.2. Obszary przetwarzania danych osobowych

1. Za obszar przetwarzania danych osobowych rozumie się przestrzeń ograniczoną fizycznymi granicami (budynek i jego wnętrze) z rozmieszczonymi w nim miejscami przetwarzania danych osobowych.
2. Miejsce przetwarzania danych to punkt, w którym zachodzą procesy przetwarzania danych osobowych, w ramach obszaru przetwarzania danych osobowych.
3. Miejsca, w których przetwarzane są dane osobowe są oznaczone w odpowiedni sposób (np. pomieszczenie służbowe)
4. Wykaz obszarów i miejsc, tworzących obszar, w którym przetwarzane są dane osobowe, uwzględnia:
   a. budynki i pomieszczenia lub części pomieszczeń, w których odbywa się przetwarzanie danych osobowych,
   b. miejsca, w których wykonuje się operacje na danych osobowych,
   c. miejsca, gdzie przechowuje się wszelkie zbiory danych oraz nośniki informacji zawierające dane osobowe,
   d. miejsca do przechowywania elektronicznych nośników informacji zawierających kopie zapasowe danych przetwarzanych w systemie informatycznym, czy też do składowania innych nośników danych,
5. Wykaz obszarów przetwarzania danych osobowych znajduje się w *Załączniku nr 6: Inwentaryzacja zasobów wspierających przetwarzanie danych osobowych* do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

5.2.1. Techniczne środki ochrony obszarów przetwarzania danych osobowych

1. Siedziba główna Biblioteki wraz z filiami chroniona jest systemem sygnalizacji włamania i napadu.
2. Parter siedziby głównej dodatkowo poddawany jest monitoringowi wewnętrznemu.

3. Budynki są wyposażone w instalację odgromową, a linie energetyczne i telekomunikacyjne są zaopatrzone w zabezpieczenia przepięciowe.
4. Pomieszczenia służbowe w obszarach przetwarzania danych osobowych, w których znajdują się stacje robocze oraz nośniki danych osobowych w postaci papierowej posiadają drzwi z zamknięciem na klucz.
5. Przeciwpożarowy wyłącznik zasilania jest umieszczony w miejscu uzgodnionym ze Strażą Pożarną, przy jednoczesnym zabezpieczeniu przed użyciem przypadkowym.
6. Pomieszczenia, w których przechowywane oraz przetwarzane są dane osobowe, w tym kluczowe elementy SI są zabezpieczone przed zniszczeniem w skutek pożaru (przy pomocy podręcznego sprzętu gaśniczego).

5.2.2. Organizacyjne środki ochrony obszarów przetwarzania danych osobowych

1. Dostęp do pomieszczeń ze zbiorami danych osobowych mają uprawnieni pracownicy.
2. Pomieszczenia w których przechowywane są dane osobowe są oznaczone znakami np. Pomieszczenie służbowe.
3. Zbiory danych osobowych oraz zbiory innych informacji znajdujące się w obszarach przetwarzania danych osobowych chronione są przez następujące zabezpieczenia: sejfy, szafy zamykane na klucz lub szyfr, zamki do pomieszczeń.
4. Na wypadek zagrożenia pożarem dla każdego obiektu Biblioteki opracowane są instrukcje przeciwpożarowe. Ciągi komunikacyjne obiektów są zaopatrzone w tabliczki informujące o kierunku ewakuacji i wyposażone w oświetlenie awaryjne.

5.3. Wymagania bezpieczeństwa dotyczące systemu informatycznego przetwarzającego dane osobowe

1. ASI odpowiedzialny jest za prowadzenie wykazu programów służących do przetwarzania danych osobowych zgodnie z *Załącznikiem nr 1: Wykaz zbiorów danych osobowych wraz ze wskazaniem programów i metod zastosowanych do przetwarzania danych osobowych* do niniejszej Polityki Bezpieczeństwa Danych Osobowych.
2. Wymagania bezpieczeństwa, zasady pracy użytkowników oraz zasady zarządzania systemami informatycznymi określa instrukcja opisana w *Załączniku nr 9: Instrukcja Zarządzania Systemami Informatycznymi Matusz, CafeSuite, Finka-FK, Finka-Płace, Płatnik oraz pakietami aplikacji biurowych* do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

6. Naruszenie bezpieczeństwa danych osobowych

W Bibliotece w celu ustalenia jednolitych zasad postępowania w przypadkach stwierdzenia naruszeń zasad ochrony przetwarzanych danych osobowych wprowadza się i utrzymuje procedury zgłaszania i obsługi zdarzeń związanych z bezpieczeństwem danych osobowych. Zasady zgłaszania zdarzeń i obsługi zdarzeń związanych z ochroną danych osobowych regulowane są instrukcją opisaną w *Załączniku nr 10: Instrukcja zgłaszania i postępowania w sytuacji naruszenia danych osobowych* do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

7. Sprawdzenia i sprawozdawczość dotycząca ochrony danych osobowych

1. Sprawdzenia realizowane są w celu:
    a. zweryfikowania zgodności przetwarzania danych osobowych z polityką bezpieczeństwa oraz z przepisami o ochronie danych osobowych,
    b. testowania zabezpieczeń, czyli sprawdzanie poprawności funkcjonowania zabezpieczeń.

2. IODO przygotowuje plan sprawdzeń. Plan sprawdzeń tworzony jest z uwzględnieniem wyników wcześniejszych sprawdzeń i innych kontroli w zakresie ochrony informacji, wyników analiz skarg i wniosków oraz zidentyfikowanego ryzyka.
3. IODO może przeprowadzać sprawdzenia przy udziale innych pracowników lub korzystać z wyspecjalizowanych przedstawicieli podmiotów zewnętrznych.
4. IODO przygotowuje sprawozdanie ze sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w Bibliotece:
    a. na podstawie zatwierdzonego planu sprawdzeń,
    b. doraźnie, jeżeli uzyskał informacje wskazujące na występowania istotnych zagrożeń dla naruszenia ochrony danych osobowych.
5. Zagadnienia objęte sprawdzeniem są zgodne z zatwierdzonym planem sprawdzeń i w zależności od przedmiotu i zakresu sprawdzenia powinny obejmować:
    a. zasady przetwarzania danych osobowych,
    b. realizację obowiązków w zakresie udzielania informacji osobom, których dane są przetwarzane,
    a. sposób zabezpieczenia danych osobowych, w szczególności:
        - zasady przechowywania danych w formie papierowej oraz elektronicznej,
        - mechanizmy kontroli dostępu do danych osobowych,
        - zastosowane środki ochrony danych osobowych przed ich utratą na skutek awarii systemu informatycznego,
        - zastosowane zabezpieczenia przed zagrożeniami pochodzącymi z sieci publicznej,
        - zastosowane zabezpieczenia przed zagrożeniami pochodzącymi z wewnętrznej sieci Biblioteki,
        - środki zapewniające poufność danych osobowych przy ich przesyłaniu w sieci publicznej oraz lokalnych urządzeń bezprzewodowych,
        - środki zapewniające poufność danych przetwarzanych przy wykorzystaniu elektronicznych przenośnych nośników informacji,
        - sposób zabezpieczenia danych przez podmiot, któremu dane zostały powierzone.
7. IODO ustala stan faktyczny na podstawie dowodów zebranych w toku sprawdzenia. Dowodami mogą być w szczególności dokumenty, oględziny, pisemne lub ustne wyjaśniania oraz utrwalone stany konfiguracji technicznych spodków zabezpieczeń.
8. Zatwierdzone przez ADO sprawozdania przechowywane są w Bibliotece zgodnie z właściwymi przepisami o archiwizacji.
9. **Corocznie do dnia 31 marca** IODO **przygotowuje sprawozdanie roczne z funkcjonowania systemu ochrony danych osobowych i przekazuje do ADO. Sprawozdanie przygotowywane jest w formie pisemnej.**
10. **Wzór sprawozdania oraz planu sprawdzeń przedstawiono w** *Załączniku nr 11: Wzór sprawozdania oraz Załączniku nr 12: Wzór planu sprawdzeń* do niniejszej Polityki Bezpieczeństwa Danych Osobowych

8. Postanowienia końcowe

Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką bezpieczeństwa i innymi związanymi z nią dokumentami obowiązującymi u administratora danych osobowych. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.

9. Załączniki

1. *Załącznik nr 1: Wykaz zbiorów danych osobowych wraz ze wskazaniem programów i metod zastosowanych do przetwarzania danych osobowych*
2. *Załącznik nr 2: Wzór zobowiązania do zachowania w poufności danych osobowych*
3. *Załącznik nr 3: Wzór upoważnienia do przetwarzania danych osobowych*
4. *Załącznik nr 4: Rejestr czynności przetwarzania danych osobowych*
5. *Załącznik nr 5: Wzór Księgi Rejestrowej*
6. *Załącznik nr 6: Inwentaryzacja zasobów wspierających przetwarzanie danych osobowych*
7. *Załącznik nr 7: Klauzula informacyjna administratora o przetwarzaniu danych osobowych*
8. *Załączniku nr 8: Szacowanie ryzyka utraty bezpieczeństwa danych osobowych*
9. *Załącznik nr 9: Instrukcja Zarządzania Systemami Informatycznymi Matusz, CafeSuite, Finka-FK, Finka-Płace, Płatnik oraz pakietami aplikacji biurowych*
10. *Załącznik nr 10: Instrukcja zgłaszania i postępowania w sytuacji naruszenia danych osobowych*
11. *Załącznik nr 11: Wzór sprawozdania*
12. *Załącznik nr 12: Wzór planu sprawdzeń*
13. *Załącznik nr 13. Plan ciągłości działania systemów informatycznych*