Załącznik nr 1 do zarządzenia nr 2/2018
Dyrektora Biblioteki Publicznej im. Z. Łazarskiego
w Dzielnicy Mokotów m.st. Warszawy
z dnia 14 grudnia 2018 r.

Polityka bezpieczeństwa danych osobowych

Biblioteki Publicznej im. Zygmunta Łazarskiego w Dzielnicy Mokotów m.st. Warszawy

wersja 3.0

1. Wstęp

Niniejszy dokument, zwany dalej *Polityką*, ustanawia podstawowe zasady przetwarzania i ochrony danych osobowych w Bibliotece Publicznej im. Zygmunta Łazarskiego w Dzielnicy Mokotów m.st. Warszawy, zwanej dalej Biblioteką, które dotyczą zarówno przetwarzania metodami tradycyjnymi, jak i w systemach informatycznych.

Każdy pracownik oraz każda inna osoba upoważniona do przetwarzania danych osobowych w Bibliotece ma obowiązek zapoznać się z postanowieniami niniejszej *Polityki* i postępować zgodnie z jej postanowieniami a także zapoznać się i postępować zgodnie z postanowieniami *Regulaminu użytkowania systemów informatycznych w Bibliotece* (zwanego dalej *Regulaminem*) oraz innych

dokumentów wchodzących w skład dokumentacji systemu ochrony danych osobowych, w zakresie, w jakim te dokumenty zostały jej udostępnione.

Zakres udostępnienia innych dokumentów wchodzących w skład dokumentacji systemu ochrony danych osobowych pracownikom oraz innym osobom upoważnionym do przetwarzania danych w Bibliotece jest uzależniony od potrzeby dostępu pracownika lub innej osoby do zawartych w tych dokumentach informacji, wynikającej z przydzielonych pracownikowi lub innej osobie obowiązków służbowych. Udostępnienie tych dokumentów następuje na podstawie decyzji Dyrektora Biblioteki, kierownika placówki lub innej komórki organizacyjnej lub Inspektora Ochrony Danych.

Informacje zawarte w niniejszej *Polityce*, *Regulaminie* oraz innych dokumentach wchodzących w skład dokumentacji systemu ochrony danych osobowych dotyczą sposobów zabezpieczenia danych osobowych w Bibliotece. Każdy, komu te informacje udostępniono zobowiązany jest do zachowania ich w tajemnicy.

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

Pod pojęciem pracownika w dokumentacji systemu ochrony danych osobowych rozumie się również osoby wykonujące prace na rzecz Biblioteki w oparciu o umowy cywilnoprawne, takie jak umowa o świadczenie usług, umowa o dzieło lub inne.

2. Podstawa prawna

- Statut Biblioteki Publicznej w Dzielnicy Mokotów m.st. Warszawy - załącznik Nr 13 do uchwały Nr XXXII/714/2004 Rady m.st. Warszawy z dnia 1 lipca 2004 r.,
- 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 (ogólne rozporządzenie o ochronie danych) zwane dalej RODO,
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 r. poz. 1000.), zwana dalej uodo.

3. Podstawowe definicje

dane osobowe - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (art. 4 pkt 1, Rozporządzenia UE nr 2016/679, zwanego dalej RODO);

przetwarzanie - 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, rozpowszechnienie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie (art. 4, pkt 2, RODO);

administrator danych – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (art. 4, pkt 7, RODO);

poufność danych - właściwość zapewniająca, że dane nie są udostępniane nieuprawnionym podmiotom lub osobom;

integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione, ani zniszczone w sposób nieuprawniony;

odbiorca – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią (art. 4, pkt 9, RODO);

strona trzecia – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe (art. 4 pkt 10, RODO);

incydent – zdarzenie lub seria zdarzeń, które mają lub mogą mieć niekorzystny wpływ na działalność Biblioteki i narażają lub mogą narazić Bibliotekę lub inne osoby na szkodę.

naruszenie ochrony danych osobowych – 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 (art. 4 pkt 12, RODO);

udokumentowane polecenie – pismo, wiadomość poczty elektronicznej, wiadomość tekstowa sms, adnotacja na dokumencie, odręczna notatka, zapis w systemie informatycznym, zarządzenie lub decyzja lub każda inna utrwalona forma przekazania polecenia służbowego pozwalająca ustalić adresata lub adresatów polecenia oraz jego autora;

4. Określenie funkcji związanych z przetwarzaniem danych osobowych

Dyrektor Biblioteki jest odpowiedzialny za wypełnienie przez Bibliotekę obowiązków ciążących na Bibliotece jako administratorze danych, w tym za zapewnienie zgodności sposobu przetwarzania i ochrony danych w Bibliotece z obowiązującymi przepisami.

Za wdrożenie i utrzymanie zabezpieczeń informatycznych, w tym za realizację zasady domyślnej ochrony danych w systemach informatycznych oraz uwzględnienia ochrony danych w fazie projektowania takich systemów, odpowiedzialny jest Administrator Systemów Informatycznych.

Za bieżące zarządzanie systemami informatycznymi Biblioteki, zapewnienie ich dostępności oraz wsparcie użytkowników odpowiedzialny jest Administrator Systemów Informatycznych. W szczególnych przypadkach bieżące zarządzanie, zapewnienie dostępności i wsparcie użytkowników w konkretnym systemem informatycznym może być delegowane na inną osobę lub podmiot wyznaczony przez Dyrektora Biblioteki.

Za wdrożenie i utrzymanie zabezpieczeń fizycznych i technicznych odpowiedzialny jest Dyrektor Biblioteki.

Za bieżące zarządzanie i nadzór nad zabezpieczeniami fizycznymi i technicznymi wdrożonymi w danej placówce odpowiedzialny jest kierownik placówki.

Za prawidłową realizację czynności przetwarzania danych osobowych w podległych im placówkach lub innych komórkach organizacyjnych odpowiedzialni są kierownicy placówek lub komórek organizacyjnych.

Za nadzór nad przestrzeganiem przepisów dotyczących przetwarzania i ochrony danych osobowych oraz nadzór nad skutecznością zabezpieczeń temu służących odpowiedzialny jest Inspektor Ochrony Danych. Do jego obowiązków należy realizowanie zadań wymienionych w art. 39 RODO, w tym:

- informowanie Dyrektora Biblioteki oraz pozostałych pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych osobowych i doradzanie im w sprawach z zakresu ochrony danych osobowych,
- monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz zasad ochrony danych osobowych określonych w dokumentacji systemu ochrony danych osobowych w Bibliotece,
- prowadzenie działań zwiększających świadomość pracowników odnośnie ochrony danych osobowych, w tym prowadzenie szkoleń oraz audytów,
- uczestniczenie w ocenie skutków dla ochrony danych osobowych i monitorowanie jej wykonania,
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego, właściwego w sprawach ochrony danych osobowych, w kwestiach związanych z przetwarzaniem danych osobowych oraz prowadzenie konsultacji we wszystkich innych kwestiach,
- pełnienie funkcji punktu kontaktowego dla osób korzystających z praw przyznanych im na mocy RODO.

Funkcję Inspektora Ochrony Danych oraz Administratora Systemów Informatycznych pełnią osoby wyznaczone przez Dyrektora Biblioteki. Informację o osobach wyznaczonych do pełnienia tych funkcji oraz o wszelkich zmianach tych osób otrzymują wszyscy pracownicy Biblioteki. W przypadku wyznaczenia nowego Inspektora Ochrony Danych, Dyrektor Biblioteki zgłasza tę zmianę organowi nadzorczemu w terminie 14 dni.

5. Zasady przetwarzania danych osobowych

Do przetwarzania danych osobowych mogą być dopuszczone tylko osoby, którym nadano pisemne upoważnienie do przetwarzania takich danych. Upoważnienia w imieniu Administratora Danych nadaje Dyrektor Biblioteki.

Zasady zarządzania upoważnieniami i uprawnieniami w systemach informatycznych opisane są w odrębnym dokumencie.

1. Obowiązki wszystkich pracowników

Pracownicy zobowiązani są stosować i w zakresie swoich kompetencji, dbać o właściwe funkcjonowanie zabezpieczeń organizacyjnych, fizycznych, technicznych i informatycznych służących ochronie danych osobowych, innych danych i informacji oraz mienia Biblioteki, wdrożonych na ich stanowisku pracy, w otoczeniu tego stanowiska oraz w całej Bibliotece.

Pracownicy zobowiązani są do nadzoru nad osobami znajdującymi się pod ich opieką (np. czytelnikami, dostawcami, kontrolerami, konserwatorami) w trakcie pobytu tych osób w Bibliotece tak, aby nie dopuścić do naruszenia przez te osoby postanowień niniejszej *Polityki* i innych dokumentów wchodzących w skład dokumentacji systemu ochrony danych osobowych.

Przebywanie osób nieupoważnionych do przetwarzania danych osobowych w obszarze przetwarzania danych osobowych, pod nieobecność osób posiadających takie upoważnienie, dozwolone jest wyłącznie wtedy, gdy nie istnieje ryzyko dostępu do danych osobowych.

Zakazane jest przetwarzanie danych osobowych bez ważnego pisemnego upoważnienia nadanego przez Administratora Danych lub wykraczające poza zakres nadanego upoważnienia. W szczególności zakazane jest przetwarzanie (w tym kopiowanie, modyfikowanie, usuwanie, udostępnianie osobom spoza Biblioteki lub innym pracownikom Biblioteki) danych osobowych lub ich zbiorów, do których dostęp pracownik uzyskał przypadkowo lub w wyniku niepoprawnej konfiguracji zabezpieczeń lub w inny nieuprawniony sposób np. w wyniku podszycia się pod innego pracownika.

2. Obowiązki osób upoważnionych do przetwarzania danych

Osoby upoważnione do przetwarzania danych osobowych mogą przetwarzać je tylko w zakresie wskazanym w nadanym im upoważnieniu oraz zgodnie z celem, dla którego dane zostały zebrane. Cele przetwarzania danych są określone w *Rejestrze czynności przetwarzania* oraz *Rejestrze kategorii czynności przetwarzania*.

Zakazane jest przetwarzanie (w tym kopiowanie, modyfikowanie, usuwanie, udostępnianie osobom spoza Biblioteki lub innym pracownikom Biblioteki) danych osobowych lub ich zbiorów z wyjątkiem:

- przetwarzania danych osobowych zgodnie z ich przeznaczeniem, opisanym w *Rejestrze czynności przetwarzania* lub *Rejestrze kategorii czynności przetwarzania* lub
- przetwarzania danych na podstawie udokumentowanego polecenia administratora danych lub
- przetwarzania danych na podstawie obowiązku wynikającego z prawa polskiego lub prawa Unii Europejskiej lub
- innych sytuacji opisanych w *Polityce bezpieczeństwa danych osobowych* lub innych dokumentach wchodzących w skład dokumentacji systemu ochrony danych osobowych (takich jak instrukcje, regulaminy, procedury) lub innych obowiązujących w Bibliotece dokumentach normatywnych.

Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobu ich zabezpieczenia, również po wygaśnięciu upoważnienia i po zakończeniu zatrudnienia w Bibliotece.

3. Zbieranie danych osobowych

Obowiązkiem osób pozyskujących nowe dane osobowe (dane nowej osoby lub nowe dane osoby, która już występuje w zbiorze) jest zapoznanie lub zapewnienie możliwości zapoznania się osoby, której te dane dotyczą z zasadami przetwarzania tych danych przez Bibliotekę, poprzez:

- użycie klauzul informacyjnych w formularzach służących do zbierania danych lub wzorach umów, oświadczeń itp. lub
- udostępnienie tych zasad w miejscu zbierania danych np. przez wywieszenie na tablicy lub na ścianie lub udostępnianie wydrukowanej informacji lub
- umieszczenie tych zasad w serwisie www Biblioteki (np. w polityce prywatności),

- zwrócenie uwagi na możliwość zapoznania się z tymi zasadami, zachęcenie do tego oraz udzielanie wyjaśnień dotyczących tych zasad.

W przypadku pozyskiwania danych osobowych z innych źródeł informacje o zasadach przetwarzania danych powinny być przekazane osobom, których dane dotyczą w drodze komunikacji z tymi osobami. Osoby pozyskujące dane w ten sposób zobowiązane są uzgodnić z Inspektorem Ochrony Danych szczegółowy sposób realizacji tego obowiązku lub możliwość wyłączenia tego obowiązku.

4. Udostępnianie danych osobowych

Udostępnianie danych przez osoby upoważnione do przetwarzania danych osobowych dopuszczalne jest, gdy:

- odbiorca danych jest na liście podmiotów lub należy do kategorii podmiotów wskazanych w *Rejestrze czynności przetwarzania* lub *Rejestrze kategorii czynności przetwarzania*, którym dane ze zbioru są udostępniane i
- w zakresie, jaki jest dla danego celu niezbędny.

Udostępnianie danych osobowych innym odbiorcom wymaga udokumentowanego polecenia administratora danych.

Odnotowanie odbiorcy oraz zakresu udostępnionych danych odbywa się w sposób określony dla danej czynności przetwarzania w odpowiednim *Rejestrze*. W przypadku, gdy odnotowanie odbiorcy ma nastąpić w *Rejestrze udostępnień*, osoba udostępniająca dane ma obowiązek powiadomić o udostępnieniu Inspektora Ochrony Danych.

6. Zarządzanie systemem ochrony danych osobowych

5. Rozliczalność i rejestrowanie czynności przetwarzania

W Bibliotece przetwarzane są zbiory danych, w stosunku do których Biblioteka posiada status administratora danych. Mogą też być przetwarzane zbiory danych, dla których administratorami danych są inne podmioty – w takim przypadku przetwarzanie odbywa się na podstawie umowy powierzenia przetwarzania danych między tymi podmiotami a Biblioteką. W obu przypadkach na tych zbiorach mogą być wykonywane różne czynności przetwarzania, o różnym celu, podstawie prawnej czy sposobie przetwarzania. Wszystkie powinny być ujęte w jednym z prowadzonych przez Bibliotekę rejestrów: *Rejestrze czynności przetwarzania* (gdy Biblioteka jest administratorem danych) lub *Rejestrze kategorii czynności przetwarzania* (gdy inny podmiot jest administratorem danych). Wyjątek stanowią czynności wykonywane jednorazowo lub sporadycznie.

Wszelkie nowe czynności lub kategorie czynności przetwarzania danych osobowych oraz istotne zmiany w istniejących czynnościach lub kategoriach czynności wymagają zgody Dyrektora Biblioteki.

Inspektor Ochrony Danych jest zobowiązany do udzielania porad i wsparcia kierownikom placówek i komórek organizacyjnych oraz pracownikom w zakresie przetwarzania i ochrony danych osobowych, zwłaszcza przy planowaniu przetwarzania i ochrony danych osobowych.

6. Wdrażanie nowych czynności przetwarzania

W przypadku potrzeby wdrożenia nowej czynności przetwarzania danych osobowych, wniosek dotyczący takiej czynności przekazywany jest przez kierownika placówki lub innej komórki organizacyjnej Dyrektorowi Biblioteki do zatwierdzenia wraz z opisem koncepcji przetwarzania danych osobowych oraz opinią Inspektora Ochrony Danych i Administratora Systemów Informatycznych, jeżeli przetwarzanie odbywać się będzie w systemie informatycznym. Rozpoczęcie przetwarzania może nastąpić dopiero po wpisaniu tej czynności do odpowiedniego *Rejestru* lub wydaniu odrębnej zgody przez Dyrektora Biblioteki (w przypadku czynności o charakterze jednorazowym lub sporadycznym).

Opinia Inspektora Ochrony Danych powinna uwzględniać m.in. następujące zagadnienia:

- istnienie podstawy prawnej dla czynności przetwarzania,
- adekwatność zakresu danych i sposób zapewnienia poprawności danych,
- sposób realizacji obowiązku informacyjnego,
- sposób realizacji uprawnień osób, których dane dotyczą,
- zidentyfikowane ryzyka dla danych osobowych wynikające z nowej czynności przetwarzania,
- sposób spełnienia wymagań dot. bezpieczeństwa danych osobowych,
- potrzebę przeprowadzenia oceny skutków dla ochrony danych.

Opinia Administratora Systemów Informatycznych powinna uwzględniać m.in. następujące zagadnienia:

- możliwość zorganizowania przetwarzania w oparciu o istniejące systemy informatyczne, sprzęt i oprogramowanie,
- niezbędne zabezpieczenia,
- harmonogram i koszt wdrożenia niezbędnych zabezpieczeń

Osoby wnioskujące o uruchomienie nowej czynności przetwarzania są zobowiązane uwzględniać wymóg tzw. domyślnej ochrony danych (oznaczającej, że dane nie są udostępniane bez wyraźnego działania uprawnionych osób) oraz ochronę danych w fazie projektowania procesów przetwarzania i systemów informatycznych wspomagających te procesy.

Wdrożenie nowej czynności przetwarzania nadzoruje Inspektor Ochrony Danych, który aktualizuje też istniejącą dokumentację systemu ochrony danych osobowych.

7. Wprowadzanie zmian w sposobie realizacji czynności przetwarzania

Wszelkie zmiany mające wpływ na przetwarzanie i ochronę danych osobowych w ramach udokumentowanych już czynności przetwarzania, zwłaszcza zmiany sposobu, zakresu, celów, miejsc, systemów i procedur przetwarzania, osoby odpowiedzialne za te czynności są zobowiązane skonsultować z Inspektorem Ochrony Danych przed ich wdrożeniem.

W przypadku gdy zmiany są istotne stosuje się odpowiednio postanowienia o wdrażaniu nowej czynności lub kategorii czynności przetwarzania. W przypadku mniej istotnych zmian wystarczające jest ich udokumentowanie, w tym w *Rejestrze czynności przetwarzania* lub *Rejestrze kategorii*

czynności przetwarzania. W razie wątpliwości czy zmiana jest istotna czy nie, decydujący głos ma Inspektor Ochrony Danych.

8. Zakończenie czynności przetwarzania

O planowanym zakończeniu przetwarzania danych osobowych osoba odpowiedzialna za daną czynność lub kategorię czynności przetwarzania zobowiązana jest poinformować Inspektora Ochrony Danych i uzgodnić procedury zakończenia przetwarzania, w tym odebrania upoważnień i uprawnień, zasady przechowywania, zwrotu lub zniszczenia danych osobowych.

Postanowienia o wdrażaniu nowej czynności lub kategorii czynności przetwarzania stosuje się odpowiednio.

9. Szacowanie ryzyka

Dyrektor Biblioteki ustala, we współpracy z Inspektorem Ochrony Danych i Administratorem Systemów Informatycznych, właściwy poziom ochrony danych osobowych, uwzględniając wyniki szacowania ryzyka.

Szacowanie ryzyka wykonywane jest przez Inspektora Ochrony Danych we współpracy z Administratorem Systemów Informatycznych, Starszym Specjalistą ds. IT i, jeżeli zachodzi taka potrzeba, kierownikami placówek lub komórek organizacyjnych. Inspektor Ochrony Danych opracowuje metodę prowadzenia szacowania ryzyka.

Szacowanie ryzyka wykonywane jest co najmniej raz w roku oraz po każdym poważnym incydencie lub naruszeniu ochrony danych osobowych a także dla każdej nowej czynności lub kategorii czynności przetwarzania danych osobowych – przed jej wdrożeniem. Szacowanie ryzyka może też być wykonane po stwierdzeniu pojawienia się nowych zagrożeń, podatności lub zabezpieczeń lub na wniosek Administratora Systemów Informatycznych lub w każdej innej sytuacji wg uznania Dyrektora Biblioteki lub Inspektora Ochrony Danych.

Wdrożenie planów postępowania z ryzykami, w tym wdrożenie nowych zabezpieczeń nadzoruje Inspektor Ochrony Danych, który aktualizuje też istniejącą dokumentację systemu ochrony danych osobowych.

10. Powierzenie przetwarzania danych osobowych

W przypadku potrzeby powierzenia przetwarzania danych osobowych Dyrektor Biblioteki odpowiedzialny jest za zawarcie w formie pisemnej lub elektronicznej umowy powierzenia przetwarzania danych, określającej m.in. cel i zakres przetwarzania danych osobowych przez podmiot zewnętrzny oraz sposób przetwarzania i zabezpieczenia powierzonych danych oraz nadzoru nad przetwarzaniem i zabezpieczeniem tych danych, a także inne elementy wymienione w art. 28 RODO.

Projekt umowy oraz uzgodnienia dot. zabezpieczeń stosowanych przez podmiot przetwarzający podlegają opiniowaniu przez Inspektora Ochrony Danych i, w przypadku, gdy powierzenie dotyczy

przetwarzania danych w systemach informatycznych Biblioteki, Administratora Systemów Informatycznych.

11. Dokumentacja systemu ochrony danych osobowych

Na dokumentację systemu ochrony danych osobowych składają się dokumenty normatywne (m.in. *Polityka bezpieczeństwa danych osobowych* i *Regulamin użytkowania systemów informatycznych*, instrukcje, procedury i standardy) oraz prowadzone na bieżąco wykazy, ewidencje i rejestry.

Politykę bezpieczeństwa danych osobowych oraz dokumenty normatywne takie jak regulaminy, instrukcje a także inne dokumenty adresowane do całego grona pracowników Biblioteki zatwierdza Dyrektor Biblioteki.

Procedury i standardy oraz inne dokumenty powstałe tylko na potrzeby administrowania systemami informatycznymi mogą być zatwierdzane przez Administratora Systemów Informatycznych po konsultacji z Inspektorem Ochrony Danych.

Instrukcje i procedury dotyczące konkretnych systemów informatycznych mogą być zatwierdzane przez Administratora Systemów Informatycznych, po konsultacji z Inspektorem Ochrony Danych, jeżeli system służy do przetwarzania danych osobowych.

Inspektor Ochrony Danych opracowuje wzorcowe klauzule informacyjne (w tym wzory klauzul do umów) i wzory umów powierzenia przetwarzania danych.

Osoby upoważnione do przetwarzania danych osobowych powinny mieć dostęp do *Polityki ochrony danych osobowych*, *Regulaminu użytkowania systemów informatycznych* oraz odpowiednich instrukcji i procedur dotyczących poszczególnych systemów informatycznych a także wzorów klauzul informacyjnych i formularzy.

Te oraz inne dokumenty są udostępniane w formie elektronicznej w serwisie www Biblioteki, w części „Dla bibliotekarzy", z zachowaniem zasady wiedzy niezbędnej.

Osoby upoważnione do przetwarzania danych osobowych powinny mieć również dostęp do *Rejestru czynności przetwarzania* oraz *Rejestru kategorii czynności przetwarzania*, przy czym, ze względu na zasadę wiedzy niezbędnej, może być to dostęp do przygotowanych przez Inspektora Ochrony Danych wyciągów z tych *Rejestrów*.

12. Przeglądy dokumentacji

Inspektor Ochrony Danych na bieżąco monitoruje zmiany aktów prawnych, przywołanych w dokumentacji systemu ochrony danych osobowych. W przypadku zmian (lub projektów zmian) sprawdza, czy mają one wpływ na system ochrony danych osobowych i jego dokumentację. W razie potrzeby informuje o zmianach osoby odpowiedzialne za czynności przetwarzania, których te zmiany dotyczą. Kierownicy komórek organizacyjnych informują Inspektora Ochrony Danych o znanych im przepisach dotyczących przetwarzania danych osobowych w ich komórkach organizacyjnych oraz o zmianach w tych przepisach.

W przypadku wprowadzenia zmian w funkcjonowaniu Biblioteki, obejmujących w szczególności:

- zmiany w aktach prawnych;
- zmiany w systemach informatycznych służących do przetwarzania danych osobowych (w tym zmianę programów lub ich wersji);
- zmiany w zabezpieczeniach organizacyjnych, fizycznych, technicznych lub teleinformatycznych;
- zmianę miejsc przetwarzania danych osobowych;
- zmianę zakresu, celu lub sposobu przetwarzania danych osobowych;
- zmianę podmiotów uczestniczących w przetwarzaniu danych osobowych w imieniu Biblioteki

Inspektor Ochrony Danych, jeżeli jest to potrzebne, przygotowuje, we współpracy z Administratorem Systemów Informatycznych i Starszym Specjalistą ds. IT oraz kierownikami komórek organizacyjnych, zaktualizowaną dokumentację i przedstawia ją do zatwierdzenia.

W przypadku zmian w dokumentacji systemu ochrony danych osobowych Inspektor Ochrony Danych informuje pracowników, których te zmiany dotyczą. Jeśli w ocenie Inspektora Ochrony Danych zachodzi taka potrzeba, odbywa się szkolenie dotyczące wprowadzonych zmian.

Raz na 2 lata Inspektor Ochrony Danych Osobowych przeprowadza przegląd całej dokumentacji systemu ochrony danych osobowych.

13. Obsługa incydentów

Wszyscy pracownicy zobowiązani są do niezwłocznego zgłaszania incydentów Administratorowi Systemów Informatycznych, kierownikowi placówki lub innej komórki organizacyjnej, Dyrektorowi Biblioteki a w przypadku gdy incydent dotyczy danych osobowych - Inspektorowi Ochrony Danych.

Przykładami incydentów dotyczących danych osobowych są:

- kradzież lub utrata nośnika zawierającego dane osobowe lub urządzenia służącego do przetwarzania danych osobowych,
- ujawnienie osobom nieuprawnionym danych osobowych np. w wyniku wysłania wiadomości poczty elektronicznej do niewłaściwych osób lub umieszczenia pliku z danymi osobowymi w miejscu dostępnym dla osób nieuprawnionych (np. na serwerze www lub na serwerze plików),
- próba pozyskania danych osobowych przez osobę nieuprawnioną, również poprzez korespondencję pocztą elektroniczną,
- nieuprawnione usunięcie (zniszczenie) danych osobowych,
- nieprawidłowa praca systemu informatycznego przetwarzającego dane osobowe, co może być wynikiem działania szkodliwego oprogramowania lub błędów w oprogramowaniu.

Jeżeli okaże się, że incydent dotyczy danych osobowych osoba, do której trafiło zgłoszenie incydentu ma obowiązek powiadomić niezwłocznie Inspektora Ochrony Danych.

Jeżeli okaże się, że incydent dotyczy systemów informatycznych osoba, do której trafiło zgłoszenie incydentu ma obowiązek powiadomić niezwłocznie Administratora Systemów Informatycznych.

Wszyscy pracownicy zobowiązani są udzielać wyjaśnień i pomocy Inspektorowi Ochrony Danych podczas analizy przyczyn i skutków incydentu.

Wszyscy pracownicy są również zobowiązani do niezwłocznego zgłaszania podejrzenia istnienia podatności (słabości) w stosowanych systemach do przetwarzania danych osobowych, w tym w stosowanych zabezpieczeniach Inspektorowi Ochrony Danych lub Administratorowi Systemów Informatycznych a w zakresie zabezpieczeń fizycznych i technicznych Inspektorowi Ochrony Danych, kierownikowi placówki lub innej komórki organizacyjnej lub Dyrektorowi Biblioteki. Zakazane są próby samodzielnego potwierdzania istnienia takiej podatności.

Zgłoszenia mogą być przekazywane telefonicznie, przy użyciu poczty elektronicznej lub osobiście a w przypadku zgłoszeń dot. incydentów w systemach informatycznych – również w systemie zgłaszania zdarzeń. W przypadku zgłoszeń złożonych za pośrednictwem systemu zgłaszania zdarzeń lub poczty elektronicznej należy telefonicznie lub osobiście powiadomić o zgłoszeniu.

Inspektor Ochrony Danych jest odpowiedzialny, w razie potrzeby we współpracy z Administratorem Systemów Informatycznych, za wyjaśnienie skutków i przyczyn zaistniałego naruszenia oraz dokonanie innych ustaleń umożliwiających ocenę stopnia ryzyka naruszenia praw i wolności osób fizycznych.

W przypadku gdy to ryzyko nie jest małe, Inspektor Ochrony Danych w uzgodnieniu z Dyrektorem Biblioteki dokonuje zgłoszenia naruszenia do organu nadzorczego.

W przypadku gdy to ryzyko jest wysokie i nie istnieją przesłanki zwalniające z tego obowiązku, Inspektor Ochrony Danych w uzgodnieniu z Dyrektorem Biblioteki przygotowuje plan powiadomienia osób, których dotknęło naruszenie oraz nadzoruje jego wykonanie.

Inspektor Ochrony Danych dokumentuje zaistniałe naruszenia.

Administrator Systemów Informatycznych jest odpowiedzialny za wyjaśnienie skutków i przyczyn zaistniałego incydentu oraz jego udokumentowanie, jeżeli nie dotyczy on danych osobowych.

Dyrektor Biblioteki może podjąć decyzję o ukaraniu pracowników winnych naruszeń lub o skierowaniu zawiadomienia o popełnieniu przestępstwa do organów ścigania.

Inspektor Ochrony Danych lub Administrator Systemów Informatycznych, każdy w zakresie swoich kompetencji, są odpowiedzialni za zaplanowanie, uzgodnienie z Dyrektorem Biblioteki i nadzorowanie wdrożenia działań naprawczych, korygujących i ew. zapobiegawczych eliminujących skutki i przyczyny zaistniałego incydentu lub naruszenia, jeżeli takich działań wymagać będzie bezpieczeństwo danych osobowych lub bezpieczeństwo systemów informatycznych.

14. Szkolenia pracowników

Pracownicy oraz inne osoby upoważnione do przetwarzania danych osobowych są szkolone przez osoby przyuczające ich na stanowisku pracy z zasad przetwarzania danych osobowych na tym stanowisku. Odbycie szkolenia jest dokumentowane w teczkach osobowych pracowników lub w innym miejscu, właściwym ze względu na sposób zatrudnienia lub współpracy osoby szkolonej.

Zakres szkolenia jest uzgadniany z Inspektorem Ochrony Danych. O ile zostanie to uznane za zasadne, szkolenia te mogą być prowadzone przez Inspektora Ochrony Danych. Szkolenia mogą odbywać się w formie *e-learningowej*.

Pracownicy oraz inne osoby upoważnione do przetwarzania danych osobowych są okresowo, nie rzadziej niż raz na 2 lata szkolone przez Inspektora Ochrony Danych z zasad ochrony danych osobowych.

15. Audyty przetwarzania danych osobowych

Inspektor Ochrony Danych co najmniej raz w roku przeprowadza planowe sprawdzenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz dokumentacją systemu ochrony danych osobowych.

Sprawdzenia powinny również uwzględniać przetwarzanie danych osobowych, których administratorem jest Biblioteka, przez podmioty, którym Biblioteka powierzyła przetwarzanie tych danych.

Z przeprowadzonego audytu sporządzane jest sprawozdanie, które jest przedstawiane Dyrektorowi Biblioteki. W przypadku wykrycia nieprawidłowości, poza zaleceniami podjęcia działań naprawczych w celu wyeliminowania skutków nieprawidłowości, Inspektor Ochrony Danych przeprowadza analizę przyczyn wykrytej nieprawidłowości i proponuje działania korygujące lub zapobiegawcze, mające na celu eliminację możliwości wystąpienia podobnych niezgodności w przyszłości.

W przypadku wykrycia niezgodności pomiędzy dokumentacją systemu ochrony danych osobowych a stanem faktycznym oraz w przypadku istnienia potrzeby przeprowadzenia działań korygujących lub zapobiegawczych Inspektor Ochrony Danych uzgadnia z Dyrektorem Biblioteki zakres, treść i harmonogram zmian w systemie ochrony danych osobowych i jego dokumentacji, nadzoruje wprowadzenie uzgodnionych zmian w życie oraz wprowadza uzgodnione zmiany w dokumentacji.

Inspektor Ochrony Danych ma prawo rekomendować Dyrektorowi Biblioteki przeprowadzenie działań lub inwestycji mających na celu poprawę bezpieczeństwa przetwarzania danych osobowych.