Polityka bezpieczeństwa 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

„Polityka bezpieczeństwa danych osobowych" określa podstawowe zasady dotyczące zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych przez Miejską i Gminną Bibliotekę Publiczną im. ks. Jana Twardowskiego w Strzelinie, które powinny być przestrzegane i stosowane podczas ich przetwarzania przez dyrekcję biblioteki oraz wszystkich pracowników i współpracowników zarówno w tradycyjnych zbiorach danych, jak i systemach informatycznych.

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 Osobowych w świetle ogólnego rozporządzenia o ochronie danych osobowych.
- Wytycznych Grupy Roboczej art. 29 dotyczących Inspektorów Danych Osobowych z dn. 13 grudnia 2016 r.
- Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych.

Definicje

RODO (rozporządzenie)	- 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.
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	- osoba (zespół osób) zatrudniona przez ADO lub współpracująca

Informatycznego (ASI)	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.
Podmiot przetwarzający	- osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu ADO.
Podmiot zewnętrzny	- osoba fizyczna lub przedsiębiorca wykonujący na rzecz Administratora Danych Osobowych prace zlecone, związane z przetwarzaniem danych osobowych oraz prace serwisowe urządzeń, na których przetwarzane są dane osobowe.
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 uprawnienia do dostępu 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.
Zbiór danych osobowych	- uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
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.
Usuwanie danych	- zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
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.
Bezpieczeństwo informacji	- zachowanie poufności, integralności i dostępności informacji.
Uwierzytelnienie	- działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
System informatyczny	- zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.
Stacja robocza	- stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom dostęp do danych znajdujących się w tym systemie.

Zakres stosowania polityki bezpieczeństwa danych osobowych

Zasady określone przez dokumentację ochrony danych osobowych mają zastosowanie do całego systemu przetwarzania danych, zarówno tradycyjnego - papierowego jak i informatycznego, a w szczególności do:

- wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych, zbiorów, wykazów, rejestrów papierowych, w których przetwarzane są lub będą informacje podlegające ochronie,
- informacji będących własnością biblioteki,
- wszystkich nośników papierowych i elektronicznych, na których są lub będą znajdować się informacje podlegające ochronie (również zapis z systemu nadzoru wizyjnego),
- wszystkich lokalizacji, budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
- wszystkich pracowników biblioteki, bez względu na funkcję i pełnione zadania, jednakże w szczególności osób, które mają dostęp do danych osobowych w ramach wypełniania obowiązków służbowych lub pełnionych zadań przy ich przetwarzaniu,

- zleceniobiorców, współpracowników, konsultantów, organów kontrolujących placówkę i innych osób mających dostęp do informacji podlegających ochronie.

Zasady dotyczące przetwarzania danych osobowych (legalność przetwarzania)

Dane osobowe muszą być:

1. Przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"). Jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.
2. Zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami („ograniczenie celu").
3. Adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych").
4. Prawidłowe i w razie potrzeby uaktualniane. Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość").
5. Przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania").
6. Przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

Obowiązki informacyjne

Dane osobowe przetwarzane w Miejskiej i Gminnej Bibliotece Publicznej im. ks. Jana Twardowskiego w Strzelinie mogą być pozyskiwane bezpośrednio od osób, których dotyczą lub z innych źródeł w granicach dozwolonych przepisami prawa.

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, zgodnie z art. 13 ust. 1 i 2 RODO, nadzorujący przetwarzanie danych (ADO) jest obowiązany poinformować tę osobę w przystępnej dla niej formie o:
   - swojej tożsamości i danych kontaktowych oraz tożsamości i danych kontaktowych swojego przedstawiciela, jeżeli istnieje,
   - danych kontaktowych Inspektora Ochrony Danych,

- celach przetwarzania, do których mają posłużyć dane osobowe,
- podstawie prawnej przetwarzania,
- prawnie uzasadnionym interesie realizowanym przez ADO lub przez stronę trzecią, jeżeli przetwarzanie odbywa się na podstawie prawnie usprawiedliwionego interesu ADO (art. 6 ust. 1 lit. f RODO),
- odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
- transferze danych do państwa trzeciego,
- okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu.
- prawie do:
  - żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą,
  - ich sprostowania, usunięcia lub ograniczenia przetwarzania,
  - wniesienia sprzeciwu wobec przetwarzania,
  - przenoszenia danych,
- prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem (jeżeli przetwarzane są dane zwykłe (art. 6 ust. 1 lit. a) RODO) lub szczególnej kategorii (art. 9 ust. 2 lit. a) RODO),
- prawie wniesienia skargi do organu nadzorczego,
- informacji, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
- informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu (art. 22 ust. 1 i 4 RODO) oraz istotnych informacjach o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. W przypadku zbierania danych osobowych z innego źródła niż od osoby, której dane dotyczą, zgodnie z art. 14 ust. 1 i 2 RODO, nadzorujący przetwarzanie danych (ADO) jest obowiązany poinformować tę osobę w przystępnej dla niej formie o:
   - informacjach z punktów wskazanych powyżej,
   - kategoriach odnośnych danych osobowych,
   - źródle pochodzenia danych osobowych, a jeżeli ma to zastosowanie, o pochodzeniu ich ze źródeł powszechnie dostępnych.

Klauzule informacyjne

Administrator Danych Osobowych powinien przekazać powyższe informacje w formie zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej oraz jasnym i prostym językiem. Obowiązek informacyjny należy spełnić na piśmie lub w inny sposób, w tym w stosownych przypadkach - elektronicznie. Wzór ogólny klauzuli informacyjnej zawarty jest w **Załączniku nr 1** do „Polityki bezpieczeństwa danych osobowych“.

Prawa osób, których dane są przetwarzane

1. Prawo do bycia poinformowanym o operacjach przetwarzania.
2. Prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych.
3. Prawo do żądania sprostowania (poprawiania) danych osobowych - w przypadku, gdy dane są nieprawidłowe lub niekompletne.
4. Prawo do żądania usunięcia danych osobowych (tzw. prawo do bycia zapomnianym) w przypadku, gdy:
   - dane nie są już niezbędne do celów, dla których były zebrane lub w inny sposób przetwarzane,
   - osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania danych osobowych,
   - osoba, której dane dotyczą wycofała zgodę na przetwarzanie danych osobowych, która jest podstawą przetwarzania danych i nie ma innej podstawy prawnej przetwarzania danych,
   - dane osobowe przetwarzane są niezgodnie z prawem,
   - dane osobowe muszą być usunięte w celu wywiązania się z obowiązku wynikającego z przepisów prawa.
5. Prawo do żądania ograniczenia przetwarzania danych osobowych w przypadku, gdy:
   - osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych,
   - przetwarzanie danych jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych, żądając w zamian ich ograniczenia,
   - Administrator nie potrzebuje już danych dla swoich celów, ale osoba, której dane dotyczą, potrzebuje ich do ustalenia, obrony lub dochodzenia roszczeń,
   - osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania danych do czasu ustalenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstawy sprzeciwu.
6. Prawo do przenoszenia danych w przypadku, gdy łącznie spełnione są następujące przesłanki:
   - przetwarzanie danych odbywa się na podstawie umowy zawartej z osobą, której dane dotyczą lub na podstawie zgody wyrażonej przez tę osobę,
   - przetwarzanie odbywa się w sposób zautomatyzowany.
7. Prawo sprzeciwu wobec przetwarzania danych w przypadku, gdy łącznie spełnione są następujące przesłanki:
   - zaistnieją przyczyny związane ze szczególną sytuacją osoby, której dane dotyczą, w przypadku przetwarzania danych na podstawie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej przez Administratora,
   - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą jest dzieckiem.
8. Prawo do tego, by nie podlegać profilowaniu.
9. W przypadku, gdy przetwarzanie danych osobowych odbywa się na podstawie zgody na przetwarzanie danych osobowych (art. 6 ust. 1 lit a RODO), prawo do cofnięcia tej zgody w dowolnym momencie. Cofnięcie to nie ma wpływu na zgodność przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, z obowiązującym prawem.

10. W przypadku powzięcia informacji o niezgodnym z prawem przetwarzaniu w placówce danych osobowych, prawo wniesienia skargi do organu nadzorczego właściwego w sprawach ochrony danych osobowych (Urzędu Ochrony Danych Osobowych).

Zasady wyrażania zgody na przetwarzanie danych osobowych

Aby przetwarzanie danych było zgodne z prawem, powinno się odbywać na podstawie:

- przepisu prawa,
- umowy zawartej z podmiotem danych,
- realizacji celów dla dobra publicznego,
- prawnie usprawiedliwionego celu Administratora Danych Osobowych, jeżeli nie narusza praw i wolności podmiotu danych,
- zgody osoby, której dane dotyczą.

Ogólne zasady wyrażania zgody na przetwarzanie danych osobowych

1. Zgoda na przetwarzanie danych wyrażana jest w celu i zakresie podanym w klauzuli informacyjnej udostępnionej osobie, której dane są przetwarzane i powinna zawierać nazwę i dane kontaktowe Administratora Danych Osobowych. Wzór ogólny klauzuli zgody na przetwarzanie danych osobowych zawarty jest w **Załączniku nr 2** do „Polityki bezpieczeństwa danych osobowych".
2. Zgoda wyrażana jest dla konkretnego administratora danych. W przypadku, gdy administrator udostępnia pozyskane dane innym administratorom (do własnych celów, np. marketingowych), powinien pozyskać odrębną zgodę. Każde udostępnienie danych powinno być odnotowywane przez administratora, aby zachować zasadę rozliczalności.
3. Zgoda powinna stanowić odrębne oświadczenie, nie może być zawarta w umowie na świadczenie usługi ani regulaminie.
4. Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele.

Zasady wyrażania zgody w bibliotece

Zgody nie wymaga:

1. Przetwarzanie danych czytelników w celu zapisania się do biblioteki i korzystania z jej zasobów (podstawą do przetwarzania danych jest konieczność zrealizowania obowiązków wynikających z ustawy o bibliotekach, z której wynika, iż czytelnik musi podać swoje dane osobowe, jeżeli chce skorzystać z usług biblioteki).
2. Publikacja imion i nazwisk laureatów konkursów organizowanych przez bibliotekę, a także wyników tych konkursów, zdobytego miejsca lub liczby uzyskanych punktów, jeśli publikację tych danych przewidywał regulamin imprezy.
3. Publikacja prac wykonanych przez uczestników zajęć organizowanych przez bibliotekę na stronie internetowej, profilach internetowych zarządzanych przez bibliotekę oraz w mediach, a także

w gazetkach i na tablicach informacyjnych, pod warunkiem, iż nie zawierają one danych osobowych w postaci imienia i nazwiska autora.
4. Upublicznianie materiałów filmowych i zdjęć osób biorących w wydarzeniach organizowanych przez bibliotekę, a także pracowników biblioteki w przypadku, gdy wizerunek osoby stanowi jedynie szczegół całości, takiej jak: zgromadzenie, krajobraz, publiczna impreza.
5. Zamieszczanie na stronie internetowej biblioteki danych obejmujących imię, nazwisko i pełnioną funkcję osób zatrudnionych w bibliotece.
6. Przetwarzanie danych pracowników biblioteki, ale tylko i wyłącznie w zakresie i celu niezbędnym do zapewnienia prawidłowego funkcjonowania placówki, zgodnie z art. 22^1 ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (t. j. Dz. U. z 2018 r. poz. 108 z późn. zm.).
7. Przetwarzanie danych osób kandydujących do pracy w celach rekrutacyjnych.

Zgoda jest wymagana w celu:

1. Przetwarzania danych uczestników imprez i wydarzeń organizowanych przez bibliotekę.
2. Upublicznienia wizerunku osób biorących udział w wydarzeniach organizowanych przez bibliotekę.
3. Przetwarzania danych pracowników biblioteki wykraczającego poza zakres i cel przewidziany przepisami prawa.
4. Wykorzystania danych osób kandydyjących do pracy w celu przyszłych rekrutacji.
5. Publikacji imion i nazwisk laureatów konkursów, a także wyników konkursów, ocen, zdobytego miejsca oraz liczby uzyskanych punktów w przypadku braku zapisów o publikacji tych danych w regulaminie imprezy.
6. Upublicznienia materiałów filmowych i zdjęć pracowników.

Udostępnianie danych osobowych

Udostępnienie innemu administratorowi, czyli przekazanie danych osobowych ma miejsce wówczas, gdy jeden administrator udostępnia dane drugiemu i każdy z tych administratorów wykorzystuje je do własnych celów. Miejska i Gminna Biblioteka Publiczna im. ks. Jana Twardowskiego w Strzelinie udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa lub za zgodą osoby, której dane dotyczą. Z mocy prawa uprawnionymi do udostępniania im danych osobowych są organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania.

Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie po pozytywnym zweryfikowaniu prawnych przesłanek dopuszczalności takiego udostępnienia. Biblioteka może odmówić udostępnienia danych osobowych, jeżeli spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą.

Każde udostępnienie danych osobowych ujęte jest w odpowiednim wykazie. Wykaz udostępnień danych innym podmiotom stanowi **Załącznik nr 3**, Wykaz udostępnień danych osobom, których dane dotyczą - **Załącznik nr 4,** natomiast wzór wniosku o udostępnienie danych osobowych - **Załącznik nr 5** do „Polityki bezpieczeństwa danych osobowych".

Powierzenie przetwarzania danych

Powierzenie przetwarzania danych osobowych ma miejsce wówczas, kiedy dane przekazane są innemu podmiotowi w celu wykonania określonych czynności przetwarzania, lecz Administratorem Danych Osobowych pozostaje nadal powierzający dane.

Powierzenie przetwarzania danych osobowych może mieć miejsce wyłącznie na podstawie pisemnej umowy określającej w szczególności:

- przedmiot przetwarzania,
- czas trwania przetwarzania,
- charakter i cel przetwarzania,
- rodzaj danych osobowych,
- kategorie osób, których dane dotyczą,
- obowiązki i prawa Administratora Danych Osobowych.

Umowa musi określać również zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy. Powierzenie przetwarzania danych osobowych musi uwzględniać wymogi wynikające z RODO. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest zobowiązany przed rozpoczęciem ich przetwarzania do:

- przestrzegania zasad zawartych w niniejszej dokumentacji ochrony danych osobowych,
- wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo i odpowiedni poziom ochrony danych.

Wymagane jest zatem, aby w umowach stanowiących podstawę powierzenia umieszczone zostały prawa Miejskiej i Gminnej Biblioteki Publicznej w Strzelinie.

Wzór umowy powierzenia stanowi **Załącznik nr 6,** wykaz podmiotów, z którymi zawarto umowy powierzenia - **Załącznik nr 7** do „Polityki bezpieczeństwa danych osobowych".

W przypadku, gdy w umowie na świadczenie usług zawartej z podmiotem przetwarzającym uwzględnione są wszystkie wymogi wynikające w RODO, nie ma konieczności sporządzania dodatkowo pisemnej umowy powierzenia.

Obowiązki Administratora Danych Osobowych

W sferze administracyjnej

1. Zapewnienie odpowiednich pomieszczeń, stosownie zabezpieczonych i wyposażonych do procesu przetwarzania i przechowywania danych osobowych.
2. Zapewnienie ciągłości stosowania odpowiednich środków technicznych i organizacyjnych oraz w razie potrzeby poddawanie ich przeglądom i uaktualnianie.
3. Wdrożenie odpowiednich procedur przetwarzania danych osobowych.
4. Weryfikowanie tożsamości osób wnoszących żądania udzielenia informacji.
5. Ułatwianie osobom, których dane są przetwarzane, wykonywanie ich praw.

W sferze pracowniczej

1. Upoważnianie pracowników do przetwarzania danych osobowych tylko w zakresie niezbędnym do wykonywania obowiązków na danym stanowisku.
2. Zaznajomienie pracowników z prawnymi oraz pracowniczymi konsekwencjami naruszenia bezpieczeństwa danych.
3. Delegowanie pracowników na okresowe szkolenia w zakresie bezpieczeństwa informacji.
4. Podział zadań i obowiązków związanych z organizacją ochrony danych osobowych, w szczególności wyznaczenie Inspektora Ochrony Danych oraz Administratora Systemu Informatycznego.

Bibliotekę jako Administratora Danych Osobowych reprezentuje dyrektor.

Obowiązki Inspektora Ochrony Danych

W obszarze administracyjnym

1. Monitorowanie przestrzegania przepisów RODO przez ADO i podmioty przetwarzające w sferze ochrony danych osobowych.
2. Informowanie ADO, podmioty przetwarzające oraz pracowników przetwarzających dane o zmianach przepisów o ochronie danych osobowych.
3. Współpraca z organem nadzorczym (Urząd Ochrony Danych Osobowych).
4. Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych w placówce.
5. Pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych.
6. Koordynacja procesu analizy i oceny ryzyka związanego z przetwarzaniem danych w placówce.
7. Koordynacja i aktywny udział w procesie reagowania na incydenty w zakresie naruszenia bezpieczeństwa danych osobowych.

W sferze pracowniczej

Przeprowadzanie szkoleń z bezpieczeństwa informacji dla wszystkich osób upoważnionych do przetwarzania danych osobowych w placówce. Szkolenia powinny być ponawiane w przypadku zmian w obowiązujących przepisach prawa, uregulowaniach wewnętrznych lub zmian środków technicznych i organizacyjnych stosowanych przez dyrektora.

W obszarze dokumentacyjnym

Prowadzenie i aktualizowanie dokumentacji ochrony danych osobowych, w tym:

- Wykazu osób, którym nadano upoważnienia do przetwarzania danych osobowych. Ewidencję tych osób stanowi **Załącznik nr 2** do „Procedur zarządzania dostępem do systemu przetwarzania danych osobowych".
- Ewidencji osób, które złożyły oświadczenie o zachowaniu poufności. Wzór oświadczenia wraz z wykazem osób stanowi **Załącznik nr 3** do „Procedur zarządzania dostępem do systemu przetwarzania danych osobowych".
- Wykazów podmiotów i osób, którym udostępniono dane. Wykazy stanowią **Załączniki nr 3** i **4** do „Polityki bezpieczeństwa danych osobowych".
- Wykazu podmiotów, z którymi zawarto umowy powierzenia przetwarzania danych osobowych w rozumieniu RODO oraz sporządzanie umów powierzenia zgodnie z obowiązującymi przepisami. Wykaz podmiotów, z którymi zawarto umowy powierzenia stanowi **Załącznik nr 7**, natomiast wzór umowy powierzenia stanowi **Załącznik nr 6** do „Polityki bezpieczeństwa danych osobowych".
- Raz do roku sporządzanie sprawozdania ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami ODO. Sprawozdanie stanowi **Załącznik nr 10** do „Polityki bezpieczeństwa danych osobowych".
- Sporządzanie zgłoszeń naruszenia ochrony danych osobowych do organu nadzorczego w przypadku incydentów oraz prowadzenia rejestru tych incydentów. Wzór zgłoszenia stanowi **Załącznik nr 1,** a rejestr incydentów - **Załącznik nr 2** do „Procedur reagowania na naruszenia ochrony danych osobowych".
- Zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony jej danych. Wzór zawiadomienia stanowi **Załącznik nr 3** do „Procedur reagowania na naruszenia ochrony danych osobowych".

Inspektor Ochrony Danych wyznaczany jest przez ADO drogą pisemnego upoważnienia (w przypadku niewyznaczenia Inspektora OD, jego funkcję pełni ADO). Wzór upoważnienia Inspektora OD stanowi **Załącznik nr 8** do „Polityki bezpieczeństwa danych osobowych".

Sprawdzenia zgodności przetwarzania danych osobowych z przepisami ODO

Inspektor OD przeprowadza co najmniej raz w roku, w terminie uzgodnionym z dyrektorem biblioteki, przeglądy przestrzegania przez użytkowników przepisów w zakresie ochrony danych osobowych, z czego sporządza odpowiednie sprawozdanie do dyrektora. Przegląd taki polega w szczególności na sprawdzeniu:

- dostępu do danych osobowych przez pracowników oraz jego zakresu,
- sposobu i zakresu udostępniania danych osobowych innym podmiotom,
- stosowania środków organizacyjnych i technicznych określonych w dokumentacji ochrony danych osobowych,
- zgodności z obowiązującymi przepisami prawa uregulowań zawartych w dokumentacji ODO oraz dostosowania procedur i instrukcji w niej zawartych do ewentualnych zmian środków technicznych i organizacyjnych w placówce.

Sprawozdanie sporządzane jest z wyszczególnieniem obszarów, w których występują zagrożenia dla bezpiecznego przetwarzania danych osobowych oraz wskazaniem metod i środków poprawy

bezpieczeństwa bądź wyeliminowania tych zagrożeń. Wzór sprawozdania ze sprawdzenia stanowi **Załącznik nr 10** do „Polityki bezpieczeństwa danych osobowych".

Sprawozdanie takie sporządzane jest również bezpośrednio po wykonaniu czynności sprawdzających w trybie sprawdzenia doraźnego, w przypadku wystąpienia incydentu naruszenia ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia.

Obowiązki Administratora Systemu Informatycznego

W zakresie systemu informatycznego

1. Administrowanie i konserwacja systemu informatycznego.
2. Nadzór nad tworzeniem kopii zapasowych przetwarzanych danych.
3. Monitorowanie poziomu bezpieczeństwa w systemie informatycznym oraz przekazywanie informacji o zagrożeniach Inspektorowi OD, a w przypadku jego nieobecności bezpośrednio ADO.
4. Kontrolowanie przestrzegania zasad bezpiecznego przetwarzania danych w systemie informatycznym przez pracowników biblioteki.
5. Aktywny udział w procesie reagowania na incydenty w zakresie bezpieczeństwa oraz usuwania ich skutków.

W sferze pracowniczej

1. Nadawanie uprawnień dla kont użytkowników systemu informatycznego zgodnie z poleceniem dyrektora.
2. Zmiana zakresu uprawnień w systemie w przypadku zmiany stanowiska służbowego lub zakresu obowiązków pracowników.
3. Odbieranie uprawnień kontom użytkowników, u których zakończył się okres zatrudnienia.
4. Przeprowadzanie instruktażu prawidłowego postępowania z systemem informatycznym dla osób nowo zatrudnionych.
5. Przeprowadzanie szkoleń z zasad bezpiecznej pracy, pozwalających unikać szkodliwego oprogramowania, a także z zasad postępowania w przypadku wykrycia lub podejrzenia działania złośliwego oprogramowania.

Administrator Systemu Informatycznego wyznaczany jest przez ADO drogą pisemnego upoważnienia (w przypadku niewyznaczenia ASI, jego funkcję pełni ADO). Wzór upoważnienia ASI stanowi **Załącznik nr 9** do „Polityki bezpieczeństwa danych osobowych".

Obowiązki osób upoważnionych do przetwarzania danych osobowych

Ochrona danych osobowych przetwarzanych w bibliotece dotyczy wszystkich osób (pracowników i współpracowników), które mają dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych tak w formie tradycyjnej, jak i za pomocą systemu informatycznego bez względu

na pełnioną funkcję służbową, zajmowane stanowisko oraz miejsce wykonywania pracy, w tym charakter stosunku pracy. Obowiązek zachowania tajemnicy istnieje również po ustaniu zatrudnienia /współpracy.

Do obowiązków osób przetwarzających dane osobowe należy:

1. Przetwarzanie danych osobowych na terenie placówki tylko w wyznaczonych do tego celu pomieszczeniach lub ich częściach.
2. Zabezpieczenie zbiorów danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w niniejszej dokumentacji.
3. Nieudzielanie informacji o danych osobowych przetwarzanych w placówce innym podmiotom, chyba, że obowiązek taki wynika z przepisów prawa.
4. Bezzwłoczne zawiadomienie Inspektora OD lub dyrektora placówki o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających dane osobowe.

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Zasady zapewniające bezpieczeństwo danych osobowych realizowane są w bibliotece poprzez zapewnienie danym osobowym cech:

- poufności - właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom,
- integralności - właściwości zapewniającej, że dane osobowe nie zostały zmienione w sposób nieautoryzowany lub nieuprawniony,
- rozliczalności - właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

W celu zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych w bibliotece wprowadza się następujące środki ochrony fizycznej i organizacyjnej:

1. Wprowadzono politykę bezpieczeństwa przetwarzania danych.
2. Wyznaczono Administratora Systemu Informatycznego.
3. Powołano Inspektora Ochrony Danych.
4. Dostęp do danych osobowych mają tylko osoby upoważnione.
5. Osoby upoważnione zostały zaznajomione z zasadami dotyczącymi ochrony danych osobowych oraz zobowiązane do zachowania ich w tajemnicy.
6. Osoby upoważnione zostały przeszkolone w zakresie ochrony danych osobowych na stanowisku pracy oraz ich bezpiecznego przetwarzania w systemie informatycznym.
7. Inspektor Ochrony Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
8. Budynki Biblioteki Centralnej oraz Filii Bibliotecznej w Nowolesiu spełniają przepisy dotyczące ochrony przeciwpożarowej. Pomieszczenia wchodzące w skład obszaru przetwarzania

zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i wyposażone w sprzęt ppoż. zgodnie z obowiązującymi przepisami.

9. Pomieszczenia, w których przetwarzane są dane osobowe, zabezpieczone są drzwiami zamykanymi na klucz. Klucze do tych pomieszczeń udostępniane są jedynie osobom upoważnionym przez dyrektora.
10. Osoby nieupoważnione mogą przebywać w obszarze przetwarzania danych wyłączenie w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
11. Dokumenty i nośniki elektroniczne zawierające dane osobowe przechowywane są w zamykanych szafach oraz w segregatorach w szafach na akta/regałach w pomieszczeniach administracyjnych biblioteki.
12. Po ustaniu przydatności dokumentacja papierowa zawierająca dane osobowe jest niszczona mechanicznie przy użyciu niszczarek dokumentów (na wyposażeniu).
13. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe przeznaczone do likwidacji, pozbawiane są wcześniej zapisu tych danych i niszczone mechanicznie w sposób uniemożliwiający ich użycie oraz odczyt, a w przypadku, gdy nie jest to możliwe, przeznaczane do utylizacji z uzyskaniem potwierdzenia zniszczenia (protokół likwidacji).
14. Monitory komputerów w pomieszczeniach administracyjnych zlokalizowane są w sposób uniemożliwiający osobom trzecim podgląd wyświetlanych danych.
15. Podczas chwilowej nieobecności na stanowisku pracy lub krótkiej przerwy w pracy, pracownicy zobowiązani są do uruchomienia wygaszacza ekranu na swojej stacji roboczej.
16. Na każdym stanowisku pracy stosuje się zasadę „czystego biurka" :
    - na biurku znajdują się dokumenty zawierające dane osobowe osób obsługiwanych w danej chwili, tylko w czasie niezbędnym do wykonania czynności służbowych, a następnie chowane są do zamykanych szaf/mebli biurowych,
    - odchodząc od biurka pracownik nie pozostawia dokumentów i nośników zawierających dane osobowe bez nadzoru,
    - po zakończeniu pracy dokumenty, nośniki z danymi oraz komputery przenośne zabezpiecza się w zamkniętych szafach/meblach biurowych.

W celu zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych, wprowadza się następujące środki sprzętowe, informatyczne i telekomunikacyjne:

1. Sprzęt komputerowy, drukarki, kserokopiarki oraz niszczarki dokumentów rozlokowane są w pomieszczeniach administracyjnych w sposób minimalizujący dostęp do nich przez osoby postronne.
2. Okablowanie sieciowe zostało rozlokowane w sposób umożliwiający bezpośredni dostęp do niego tylko z pomieszczeń zamykanych na klucz.
3. Zastosowano urządzenie typu UPS chroniące newralgiczne urządzenia systemu informatycznego służące do przetwarzania danych osobowych przed skutkami awarii zasilania.
4. Na serwerze i wszystkich stanowiskach służących do przetwarzania danych osobowych zastosowano oprogramowanie antywirusowe z codzienną aktualizacją bazy sygnatur wirusów.

5. Udostępnienie użytkownikom systemu informatycznego zasobów zawierających dane osobowe następuje na podstawie uprawnień w systemie nadanych przez Administratora Danych Osobowych.
6. Dostęp do zasobów zawierających dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła zabezpieczającego.
7. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbiorów danych osobowych.
8. Hasła zabezpieczające składają się z minimum 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne.
9. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności użytkownika.
10. Zastosowano cykliczne tworzenie kopii zapasowych w celu ochrony danych osobowych przed utratą.

Postanowienia końcowe

1. Niniejsza „Polityka bezpieczeństwa danych osobowych“ powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w placówce, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.
2. Zmiany niniejszej „Polityki bezpieczeństwa danych osobowych“ wymagają przeglądu innych dokumentów dotyczących ochrony danych osobowych obowiązujących w placówce.
3. W wypadku odrębnych od zawartych w dokumentacji uregulowań występujących w innych procedurach lub dokumentach, użytkownicy systemu mają obowiązek stosowania zapisów, o wyższym poziomie ochrony danych osobowych.
4. Użytkownicy systemu zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej dokumentacji ochrony danych osobowych.
5. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej dokumentacji ochrony danych osobowych mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, co niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, może być podstawą do wyciągnięcia wniosków dyscyplinarnych wobec osoby, która dopuściła się ich naruszenia.
6. Wobec osoby, która w przypadku naruszenia zasad bezpieczeństwa lub uzasadnionego domniemania takiego naruszenia nie podjęła działań określonych w niniejszej dokumentacji, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

Załączniki

Załącznik nr 1	- Klauzula informacyjna - wzór ogólny.
Załącznik nr 2	- Klauzula zgody - wzór ogólny.
Załącznik nr 3	- Wykaz udostępnień danych innym podmiotom.
Załącznik nr 4	- Wykaz udostępnień danych osobom, których dotyczą.
Załącznik nr 5	- Wniosek o udostępnienie danych osobowych.
Załącznik nr 6	- Umowa powierzenia przetwarzania danych.
Załącznik nr 7	- Wykaz podmiotów, z którymi zawarto umowy powierzenia.
Załącznik nr 8	- Upoważnienie Inspektora OD.
Załącznik nr 9	- Upoważnienie Administratora Systemu Informatycznego.
Załącznik nr 10	- Sprawozdanie ze sprawdzenia zgodności przetwarzania danych z przepisami ODO.