

## Zarządzenie Nr 10/2011

### Dyrektora Biblioteki Publicznej Gminy Kozienice

im. ks. Franciszka Siarczyńskiego w Kozienicach  
z dnia 22 listopada 2011 r.

#### **w sprawie ochrony danych osobowych i baz danych w systemach informatycznych i tradycyjnych w Bibliotece Publicznej Gminy Kozienice**

Działając na podstawie § 10 Statutu Biblioteki Publicznej Gminy Kozienice im. Ks. F. Siarczyńskiego nadanego uchwałą Rady Miejskiej w Kozienicach Nr XXXI/514/2005 w sprawie zmiany nazwy i nadania statutu Bibliotece Publicznej Gminy Kozienice, art. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity z 2002 r.: Dz. U. Nr 101, poz. 926 z późniejszymi zmianami) w związku z § 1 i § 9 rozporządzenia 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. Nr 100, poz. 1024) zarządzam co następuje:

#### § 1

Przetwarzanie danych osobowych w Bibliotece Publicznej Gminy Kozienice, zwanej dalej Biblioteką służy realizacji zadań wynikających z ustawy z dnia 27 czerwca 1997 r. o bibliotekach.

#### § 2

Ustalam wytyczne polityki bezpieczeństwa danych osobowych przetwarzanych w Bibliotece w związku z realizacją jej celów statutowych w brzmieniu załącznika nr 1 do Zarządzenia.

#### § 3

1. Administratorem danych osobowych w rozumieniu ustawy o ochronie danych osobowych jest Biblioteka.
2. Osobą odpowiedzialną za całokształt zarządzania bezpieczeństwem informacji jest Dyrektor Biblioteki.
3. Obowiązki wynikające z ustawy o ochronie danych osobowych powierzam:
  - 1) Specjaliście ds. organizacyjno-administracyjnych w zakresie danych osobowych pracowników Biblioteki
  - 2) Kierownikowi ds. merytorycznych w zakresie nadzoru nad realizacją ustawy w odniesieniu do czytelników w placówkach bibliotecznych
  - 3) Bibliotekarzom w placówkach w odniesieniu do użytkowników ich placówek
4. Ustalam, że osobą odpowiedzialną za bezpieczeństwo danych osobowych w Bibliotece, zwaną dalej „administratorem bezpieczeństwa informacji” (ABI) jest Informatyk - Administrator sieci komputerowej.
5. ABI wykonuje zadania ochrony danych osobowych zgodnie z przepisami ustawy o ochronie danych osobowych oraz wynikające z rozporządzenia Ministra Spraw Wewnętrznych i Administracji z pomocą pracowników wymienionych w ust 2.
6. Baza danych zawierająca dane osobowe czytelników obsługiwanych w programie bibliotecznym ALEPH jest rejestrowana na serwerze zlokalizowanym w Bibliotece Głównej Województwa Mazowieckiego w Warszawie, ul. Koszykowa 26/28 i jest tam przetwarzana dla celów statystycznych.
7. Baza danych zawierająca dane osobowe czytelników obsługiwanych w programie bibliotecznym KOHA jest rejestrowana na serwerze zlokalizowanym w siedzibie Biblioteki i jest tam przetwarzana dla celów statystycznych.

#### § 4

1. Administrator bezpieczeństwa informacji prowadzi dokumentację odzwierciedlającą wykonywanie zadań z zakresu ochrony danych osobowych i baz danych:
  - a) ewidencję baz danych, w których przetwarzane są dane osobowe w Bibliotece, zgodnie z zał. nr 2 do niniejszego zarządzenia,

- b) ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych, zgodnie z zał. nr 3 do niniejszego zarządzenia,
  - c) ewidencję miejsc przetwarzania danych osobowych w Bibliotece i sposobu ich zabezpieczania, zgodnie z zał. nr 4 do niniejszego zarządzenia.
2. Specjalistę ds. organizacyjno-administracyjnych zobowiązuje do uzupełnienia akt osobowych pracowników Biblioteki zatrudnionych przy przetwarzaniu danych osobowych o:
    - a) imienne zaświadczenia o prawie dostępu do systemu informatycznego, w którym przetwarzane są dane osobowe, wydane przez Dyrektora.
    - b) zobowiązanie – w zakresie obowiązków – dotyczące indywidualnej odpowiedzialności za przestrzeganie przepisów o ochronie danych osobowych,
    - c) zobowiązanie o zachowaniu w tajemnicy zasad bezpieczeństwa danych osobowych stosowanych w czasie ich przetwarzania, nawet po ustaniu stosunku pracy,
    - d) oświadczenia, z których wynika, że zapoznali się z aktualnymi przepisami dotyczącymi ochrony danych osobowych.
  3. Termin realizacji zadań określonych w ust. 1 i 2 ustalam do końca br.
  4. Udostępnienie danych osobowych pracowników i czytelników Biblioteki do celów innych niż określone w § 1 niniejszego zarządzenia, odbywa się wyłącznie za pośrednictwem Specjalisty ds. organizacyjno-administracyjnych w przypadku pracowników i Kierownika ds. merytorycznych w przypadku czytelników (dotyczy wszystkich placówek), po uprzednim uzyskaniu zgody Dyrektora.
  5. Na wniosek osoby, której dane dotyczą, administrator danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji, o których mowa w art. 32 ust. 1 ustawy

#### § 5

Szczegółowe zasady ochrony danych osobowych i baz danych przetwarzanych w zbiorach danych Biblioteki zawarte zostały w Instrukcjach określających sposób zarządzania i formy zabezpieczeń systemów informatycznych, służących do przetwarzania danych osobowych w Bibliotece, stanowiących zał. nr 5 i 5a do niniejszego zarządzenia,

#### § 6

Pracownicy Biblioteki zobowiązani są do przestrzegania przepisów ustawy o ochronie danych osobowych, w szczególności poprzez:

- 1) znajomość i stosowanie w pracy wytycznych polityki bezpieczeństwa danych osobowych przetwarzanych w Bibliotece, które są zamieszczone w załączniku nr 1 do zarządzenia
- 2) wdrożenie i przestrzeganie instrukcji, będących załącznikiem nr 5 i 5a do niniejszego zarządzenia,
- 3) stworzenie warunków odpowiednich do spełnienia wymogów wynikających z ustawy o ochronie danych osobowych na ich stanowiskach pracy.
- 4) wykonywanie zaleceń administratora bezpieczeństwa informacji w Bibliotece w zakresie ochrony danych osobowych i baz danych funkcjonujących w ich placówkach.

#### § 7

Osoby nie przestrzegające przepisów w zakresie ochrony danych osobowych podlegają sankcjom przewidzianym w rozdziale 8 ustawy o ochronie danych osobowych.

#### § 8

Zarządzenie wchodzi w życie z dniem podpisania, zastępując dotychczasowe uregulowania w zakresie ochrony danych osobowych, obowiązujące od 02.01.2012 r.

#### § 9

Zarządzenie podlega publikacji w BIP.

## **Polityka bezpieczeństwa danych osobowych w Bibliotece Publicznej Gminy Kozienice**

### **1. Wstęp**

Niniejszy dokument stanowi zestaw obowiązujących zasad i dobrych praktyk regulujących sposób przetwarzania i ochrony danych osobowych w Bibliotece Publicznej Gminy Kozienice (zwanej dalej Biblioteką) zarówno metodami tradycyjnymi, jak i w systemach informatycznych.

Wszyscy pracownicy oraz inne osoby upoważnione do przetwarzania danych osobowych w Bibliotece mają obowiązek zapoznania się z postanowieniami niniejszej polityki i postępowania zgodnie z jej postanowieniami a także zapoznania się i postępowania zgodnie z postanowieniami instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Bibliotece oraz innych dokumentów wchodzących w skład dokumentacji systemu ochrony danych osobowych, w zakresie, w jakim te instrukcje i dokumenty zostały im udostępnione.

Informacje zawarte w niniejszej polityce, instrukcjach zarządzania systemami informatycznymi oraz innych dokumentach wchodzących w skład dokumentacji systemu ochrony danych osobowych dotyczą sposobów zabezpieczenia danych osobowych w Bibliotece. Pracownicy oraz inne osoby, którym te informacje udostępniono zobowiązane są do zachowania ich w tajemnicy.

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

### **2. Podstawa prawna**

- Statut Biblioteki Publicznej Gminy Kozienice im. Ks. F. Siarczyńskiego nadany uchwałą Rady Miejskiej w Kozienicach Nr XXXI/514/2005 w sprawie zmiany nazwy i nadania statutu Bibliotece Publicznej Gminy Kozienice.
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 Nr 133 póź. 883) z późniejszymi zmianami, zwana dalej uodo.
- 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 póź. 1024), zwane dalej Rozporządzeniem.

### **3. Podstawowe definicje**

**dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (art. 6, uodo);

**przetwarzanie danych** - jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych (art. 7, pkt. 2. uodo);

**poufność danych** - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;

**integralność danych** - właściwość zapewniająca, że dane osobowe nie zostały zmienione, ani zniszczone w sposób nieautoryzowany;

**rozliczalność danych** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

**odbiorca danych** - każdy, komu udostępnia się dane osobowe z wyłączeniem: osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela o którym mowa w art. 31a, podmiotu o którym mowa w art. 31 (podmiotu, któremu powierzono dane), organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem (art. 7, pkt. 6, uodo);

**udostępnianie danych** - przekazywanie (w dowolnej formie: pisemnej, ustnej, poprzez umożliwienie wglądu) danych osobowych (nawet pojedynczych). Przekazywanie danych odbiorcom danych wymaga odnotowania.

### **4. Wykaz zbiorów danych osobowych i programów stosowanych do przetwarzania tych danych**

W Bibliotece przetwarzane są zbiory danych, w stosunku do których Biblioteka posiada status administratora danych.

Biblioteka może powierzyć przetwarzanie danych osobowych innym podmiotom - w takim przypadku przetwarzanie odbywa się na podstawie umowy powierzenia przetwarzania danych między Biblioteką a tymi podmiotami.

Szczegółowy wykaz zbiorów danych, zawierający charakterystykę tych zbiorów oraz opis przepływów danych pomiędzy systemami informatycznymi służącymi do przetwarzania tych zbiorów znajduje się w odrębnym dokumencie. Zasady tworzenia nowych zbiorów, wprowadzania zmian w sposobie przetwarzania lub ochrony istniejących zbiorów oraz wycofywania zbiorów z eksploatacji opisane są w rozdziale 6.

## **5. Zasady przetwarzania danych osobowych**

### **5.1 Określenie osób pełniących funkcje związane z przetwarzaniem i ochroną danych**

Dyrektor Biblioteki jest odpowiedzialny za wypełnienie przez Bibliotekę ustawowych obowiązków ciążących na Bibliotece jako administratorze danych.

Dyrektor Biblioteki wyznacza osoby administrujące poszczególnymi zbiorami danych. Osoby te są odpowiedzialne za zapewnienie zgodności sposobu przetwarzania i ochrony danych w zbiorze z obowiązującymi przepisami.

Za wdrożenie i utrzymanie zabezpieczeń teleinformatycznych odpowiedzialny jest Administrator bezpieczeństwa informacji (ABI).

Za wdrożenie i utrzymanie zabezpieczeń fizycznych i technicznych odpowiedzialny jest Specjalista ds. organizacyjno-administracyjnych.

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

Zgodę na przebywanie osób nieupoważnionych w obszarze przetwarzania danych osobowych pod nieobecność osób upoważnionych do przetwarzania tych danych mogą wydawać w imieniu Administratora danych: Dyrektor, Kierownik ds. merytorycznych, ABI.

### **5.2 Obowiązki osób upoważnionych do przetwarzania danych osobowych**

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 *Wykazie zbiorów danych osobowych*.

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

- sytuacji opisanych w polityce bezpieczeństwa lub instrukcjach zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych lub
- przetwarzania danych osobowych zgodnie z ich przeznaczeniem lub
- przetwarzania danych na podstawie pisemnej decyzji Dyrektora.

Wprowadzenie do zbioru danych osobowych nowej osoby możliwe jest dopiero po poinformowaniu jej o adresie i pełnej nazwie administratora danych, celu przetwarzania (w tym odbiorcach lub kategoriach odbiorców), prawie dostępu do treści i poprawiania danych oraz dobrowolności lub obowiązku podania danych. Wyjątek stanowią sytuacje, gdy osoba, której dane dotyczą powyższe informacje już posiada. W przypadku zbierania danych za pośrednictwem osób trzecich, konieczne jest poinformowanie osoby, której dane dotyczą o adresie i pełnej nazwie administratora danych, celu i zakresie zbierania danych, źródle danych, prawie dostępu do treści i poprawiania danych oraz o uprawnieniach zakazowych (z art. 32 ust. 7 i 8). Poinformowanie może być ustne. Załącznik 1 zawiera wzory informacji udzielanych osobom, których dane są zbierane.

Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do zachowania szczególnej staranności w celu zachowania poufności i integralności przetwarzanych danych osobowych.

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

Osoby upoważnione do przetwarzania danych osobowych mają obowiązek uwierzytelniać się w systemie informatycznym służącym do przetwarzania danych osobowych za pomocą swojego identyfikatora i hasła. Zakazane jest udostępnianie identyfikatora i hasła zezwalającego na dostęp i przetwarzanie danych osobowych

innym osobom. Zakazane jest udostępnianie stacji roboczej podczas otwartej sesji dostępu lub przetwarzania danych osobowych innym osobom (również upoważnionym pracownikom Biblioteki).

Zakazane jest udostępnianie komputerów (stacji roboczych) osobom niebędącym pracownikami Biblioteki (również w przypadku zamkniętej sesji dostępu). Wyjątek stanowią osoby wykonujące czynności na rzecz Biblioteki, będące w towarzystwie Informatyka.

### **5.3 Obowiązki wszystkich pracowników**

Wszyscy pracownicy zobowiązani są do przestrzegania postanowień niniejszej dokumentacji systemu ochrony danych osobowych. W szczególności zobowiązani są stosować i, w zakresie swoich kompetencji, dbać o właściwe funkcjonowanie środków organizacyjnych i technicznych służących ochronie danych osobowych, wdrożonych na ich stanowisku pracy, w otoczeniu tego stanowiska oraz w całej Bibliotece.

Przebywanie pracowników nieupoważnionych do przetwarzania danych osobowych w obszarze przetwarzania danych osobowych, pod nieobecność pracowników posiadających takie upoważnienie, dozwolone jest wyłącznie za zgodą Dyrektora, Kierownika ds. merytorycznych lub ABI.

Zakazane jest przetwarzanie danych osobowych bez ważnego pisemnego upoważnienia nadanego przez Dyrektora Biblioteki.

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 sposób niepoprawnej konfiguracji mechanizmów kontroli dostępu lub w sposób nieuprawniony - np. w wyniku podszycia się pod pracownika upoważnionego do przetwarzania danych osobowych.

Zakazane jest przetwarzanie (w tym przechowywanie) danych osobowych w systemach informatycznych Biblioteki w innych zbiorach niż określone w wykazie zbiorów danych osobowych.

Zakazane są wszelkie działania skutkujące połączeniem systemów informatycznych Biblioteki przetwarzających dane osobowe do sieci publicznej lub innych sieci zewnętrznych podejmowane bez zgody ABI.

Wszyscy pracownicy zobowiązani są do niezwłocznego zgłaszania incydentów związanych z danymi osobowymi a także podejrzenia istnienia podatności (słabości) w stosowanych systemach do przetwarzania danych osobowych: ABI i Dyrektorowi lub Kierownikowi ds. merytorycznych, a w zakresie zabezpieczeń fizycznych i technicznych – Specjaliście ds. organizacyjno-administracyjnych. Zakazane są próby samodzielnego potwierdzenia istnienia takich podatności.

Wszyscy pracownicy zobowiązani są do nadzoru nad osobami znajdującymi się pod ich opieką (np.: dostawcami, czytelnikami, kontrolerami) w trakcie pobytu w Bibliotece tak, aby nie dopuścić do naruszenia przez te osoby postanowień niniejszej dokumentacji systemu ochrony danych osobowych.

### **5.4 Udostępnianie danych osobowych**

#### **5.4.1 Udostępnianie w celu włączenia do zbioru**

Dozwolone jest udostępnianie danych przez osoby upoważnione do przetwarzania danych osobowych w celu włączenia do zbioru w przypadku, gdy:

- odbiorca danych figuruje na liście podmiotów, którym dane ze zbioru są udostępniane i
- w zakresie, jaki jest dla danego celu niezbędny.

Odnotowanie faktu udostępnienia, odbiorcy oraz zakresu udostępnianych danych odbywa się przy użyciu systemu informatycznego, zgodnie z postanowieniami odpowiednich *Instrukcji zarządzania systemem informatycznym*.

Udostępnianie danych osobowych w celu włączenia do zbioru odbiorcom innym niż wymienieni dla danego zbioru w wykazie zbiorów danych osobowych wymaga decyzji Dyrektora Biblioteki.

#### **5.4.2 Udostępnianie w celu innym niż włączenie do zbioru**

Pracownicy przetwarzający dane osobowe mają prawo udostępnić dane tylko za zgodą Dyrektora Biblioteki.

Dyrektor Biblioteki udostępnia dane w celu innym niż włączenie do zbioru zgodnie z art. 29 ustawy o ochronie danych osobowych. Dane osobowe udostępniane są na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej.

Wnioski i polecenia Dyrektora są przechowywane u Kierownika ds. merytorycznych dla wszystkich placówek. Do każdego wniosku dołączana jest notatka dotycząca sposobu załatwienia danego wniosku.

Podczas rozpatrywania wniosku o udostępnienie danych (z wyjątkiem wniosków, dla których podstawę stanowi art. 29, ust. 1 uodo), ABI wstępnie opiniuje wniosek. Ma on obowiązek sprawdzić, czy nie wpłynął sprzeciw z art. 32 ust. 1 pkt 8 uodo wobec udostępnienia danych wnioskującemu podmiotowi. Sprzeciwy są odnotowywane zgodnie z punktem 5.5. Jeśli sprzeciw wpłynął, należy go uwzględnić przy wydawaniu opinii. Opinia wraz z wnioskiem jest przekazywana Dyktorowi Biblioteki, który wydaje decyzję dotyczącą udostępnienia danych.

W przypadku podjęcia decyzji o odmowie udostępnienia danych wnioski, z adnotacją o decyzji, są przechowywane Kierownika ds. merytorycznych dla wszystkich placówek.

#### **5.4.3 Udostępnianie danych na wniosek osoby, której dane dotyczą**

Na pisemną prośbę pracownika Biblioteki o udostępnienie jego danych (w prośbie zawarte jest określenie podmiotu, któremu należy udostępnić dane, cel udostępnienia i zakres udostępnianych danych), Dyrektor Biblioteki może udostępnić wskazane dane w formie pisemnej. Pisemna prośba pracownika z adnotacją dotyczącą sposobu załatwienia sprawy jest przechowywana wraz z innymi wnioskami o udostępnienie danych. Udostępnienie danych (również potwierdzenie) przez telefon nie jest dozwolone, chyba, że pracownik w złożonej przez siebie pisemnej prośbie, określi imię i nazwisko oraz numer telefonu osoby, której należy udostępnić (lub potwierdzić) dane. W takim przypadku dopuszczalne jest udostępnienie danych przez telefon wskazanej osobie, pod warunkiem, że to pracownik Biblioteki zadzwoni pod wskazany numer telefonu.

#### **5.5 Realizacja obowiązków informacyjnych, korekcyjnych i zakazowych z art. 32-35 ustawy o ochronie danych osobowych**

Pracownicy upoważnieni do przetwarzania danych osobowych mają obowiązek (nie częściej niż raz na 6 miesięcy) umożliwiać kontrolę przetwarzania własnych danych osobowych przez osobę, której dane dotyczą. W szczególności informować (w terminie 30 dni od otrzymania zapytania), w jakich zbiorach danych dane są przetwarzane, kto jest administratorem danych, jaki jest adres siedziby administratora oraz informować o celu, zakresie i sposobie przetwarzania danych osobowych, od kiedy dane tej osoby są przetwarzane i jaka jest treść danych, udzielać informacji o źródle pochodzenia danych oraz o sposobie udostępniania danych (odbiorcach i kategoriach odbiorców, którym dane są udostępniane).

W przypadku zbiorów przetwarzanych w systemach informatycznych, miejsca odnotowywania informacji o źródle danych oraz o odbiorcach opisane są w odpowiednich *Instrukcjach zarządzania systemami informatycznymi*.

Dopóki dane czytelników w niektórych placówkach są przetwarzane w postaci papierowej, informacje o udostępnieniach odnotowywane na zobowiązaniach czytelników. Pracownik Biblioteki udzielający informacji o przetwarzaniu danych ma obowiązek zweryfikować, czy dane osoby, która wystąpiła z prośbą o informacje, są przetwarzane w pozostałych lokalizacjach Biblioteki i uwzględnić zebrane informacje w odpowiedzi zgodnie z formularzem przedstawionym w Załączniku 1.

Na żądanie osoby, której dane dotyczą, w przypadku niekompletności, nieprawdziwości lub nieaktualności danych, pracownicy upoważnieni do przetwarzania danych są zobowiązani do ich aktualizacji, zapewnienia kompletności i prawdziwości. Wniosek o korektę danych powinien mieć postać pisemną (np. potwierdzenie aktualnych danych podpisem i datą na zobowiązaniu czytelnika). Pracownik przed dokonaniem korekty powinien sprawdzić prawdziwość nowych danych. W przypadku aktualizacji danych, jeśli to konieczne, pracownik dokonujący aktualizacji danych powinien poinformować administratorów danych, którym udostępniono te dane.

W przypadku, gdy dane są zbędne do realizacji celu, dla którego zostały zebrane, pracownicy upoważnieni do przetwarzania danych zobowiązani są do ich usunięcia. Dane powinny zostać zniszczone w taki sposób by zapewnić anonimizację zawartej w nich informacji np. poprzez pocięcie w niszczarce lub spalenie.

W przypadku wniesienia sprzeciwu wobec przetwarzania danych osobowych na podstawie art. 32 ust. 1 pkt 7 i 8. O wniesieniu sprzeciwu informowany jest ABI. Sprzeciw taki i jego zakres zostaje odnotowany w systemie informatycznym w miejscach wskazanych w odpowiednich *Instrukcjach zarządzania systemem informatycznym*. Dopóki dane czytelników są przetwarzane w postaci papierowej, w przypadku braku możliwości odnotowania sprzeciwu w systemie informatycznym, sprzeciw czytelnika może być odnotowany na jego zobowiązaniu.

Jeśli przesłanką legalizującą przetwarzanie danych jest art. 23 ust. 1, pkt 4 (przetwarzanie jest niezbędne do wykonywania określonych prawem zadań realizowanych dla dobra publicznego) albo art. 23 ust. 1, pkt 5 (przetwarzanie jest niezbędne do wypełnienia prawnie usprawiedliwionych celów administratora danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą), Dyrektor Biblioteki podejmuje decyzję o zaprzestaniu przetwarzania danych do celów objętych sprzeciwem. Jeśli sprzeciw dotyczy udostępniania danych innym administratorom danych, wówczas Dyrektor Biblioteki nie udostępnia danych osoby z wyjątkiem przypadków określonych w art. 29 ust. 1. uodo.

Przed udzieleniem informacji dotyczącej danych osobowych, skorygowaniem danych lub ich usunięciem na wniosek osoby, której dane dotyczą należy zweryfikować tożsamość tej osoby. Wszelkie pisemne wnioski wraz z adnotacją dotyczącą sposobu załatwienia sprawy należy przekazać Kierownika ds. merytorycznych w celu przechowywania.

## **6. Zarządzanie systemem ochrony danych osobowych**

### **6.1 Dokumentacja systemu ochrony danych osobowych**

Na dokumentację systemu ochrony danych osobowych składają się następujące dokumenty:

- polityka bezpieczeństwa danych osobowych
- instrukcje zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych
- procedury zarządzania upoważnieniami i uprawnieniami
- wykaz zbiorów danych osobowych
- specyfikacja obszaru przetwarzania danych osobowych oraz wykaz środków organizacyjnych i technicznych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Za utrzymanie i właściwe udostępnianie dokumentacji odpowiedzialny jest ABI.

Politykę bezpieczeństwa danych osobowych, instrukcje zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych i instrukcje użytkowania tych systemów zatwierdza Dyrektor Biblioteki po uzyskaniu opinii osoby administrującej zbiorem, którego dotyczy instrukcja.

Pozostałe dokumenty zatwierdza Informatyk.

Każda placówka Biblioteki posiada kopię polityki ochrony danych osobowych i odpowiednich instrukcji użytkowania oraz zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych. Kopie potwierdzane są na zgodność z oryginałem przez Informatyka. Dokumenty mogą być również udostępnione w wewnętrznej sieci komputerowej Biblioteki, pod warunkiem zabezpieczenia dostępu do nich (w tym zabezpieczenia przed nieuprawnioną modyfikacją), odpowiadającego zasadom dostępności dokumentów papierowych.

### **6.2 Przeglądy dokumentacji**

Informatyk raz na 6 miesięcy przeprowadza przegląd aktów prawnych, powołanych w dokumentacji systemu ochrony danych osobowych. W przypadku zmian sprawdza, czy mają one wpływ na system ochrony danych osobowych i jego dokumentację. W razie potrzeby informuje o takich zmianach osoby administrujące zbiorami, których te zmiany dotyczą. Wspólnie z tymi osobami uzgadnia zakres, treść i harmonogram zmian w systemie ochrony danych osobowych i jego dokumentacji, nadzoruje wprowadzanie uzgodnionych zmian w życie oraz wprowadza uzgodnione zmiany w dokumentacji.

Informatyk raz na rok przeprowadza przegląd dokumentacji systemu ochrony danych osobowych pod względem adekwatności do organizacji pracy. W razie potrzeby dokonuje aktualizacji dokumentacji.

### **6.3 Zmiany w dokumentacji systemu ochrony danych osobowych**

Wszelkie zmiany w dokumentacji systemu ochrony danych osobowych wymagają formy pisemnej. Nowy dokument jest oznaczany nowym numerem wersji, datą, od której zaczyna obowiązywać oraz datą zatwierdzenia i podpisem osoby zatwierdzającej.

Pracownicy Biblioteki są informowani za pomocą poczty elektronicznej lub na wewnętrznym spotkaniu pracowników o zmianie dokumentacji systemu ochrony danych osobowych.

W przypadku konieczności wprowadzenia zmian informacji określonych w art. 41 uodo, Informatyk przygotowuje zgłoszenie aktualizacyjne zbioru danych czytelników i przedkłada je Dyrektorowi Biblioteki do zatwierdzenia. Po zatwierdzeniu wysyła wniosek listem poleconym do Biura GODO pozostawiając sobie kopie wniosku z załączonym potwierdzeniem nadania lub zawozi wniosek osobiście i potwierdza wpływ dokumentu do Biura GODO na kopii dokumentu. Kopia wniosku aktualizującego i potwierdzenie dostarczenia wniosku są przechowywane przez Kierownika ds. merytorycznych.

## **6.4 Zarządzanie zbiorami danych osobowych**

### **6.4.1 Tworzenie nowego zbioru danych osobowych**

W przypadku potrzeby utworzenia nowego zbioru danych i przetwarzania go w systemie elektronicznym wniosek o wprowadzenie do eksploatacji nowego zbioru przekazywany jest Dyrektorowi Biblioteki wraz z opisem koncepcji przetwarzania danych osobowych oraz opinią ABI i opinią Specjalisty ds. organizacyjno-administracyjnych.

Osoba administrująca nowym zbiorem zobowiązana jest ustalić we współpracy z ABI właściwy poziom ochrony danych. Jeżeli zachodzi potrzeba wdrożenia nowych zabezpieczeń za ich wdrożenie i eksploatację odpowiada ABI i Specjalista ds. organizacyjno-administracyjnych.

Na wniosek ABI Dyrektor Biblioteki aktualizuje dokumentację przetwarzania danych w związku z utworzeniem nowego zbioru. W razie potrzeby dokonywana jest rejestracja zbioru.

Rozpoczęcie przetwarzania danych w zbiorze (zbierania danych) następuje po wdrożeniu właściwego poziomu ochrony oraz dokonaniu czynności rejestracyjnych<sup>1</sup>, o ile takie są potrzebne.

### **6.4.2 Wprowadzanie zmian w sposobie przetwarzania i ochrony zbioru danych osobowych**

O planowanych zmianach w systemie przetwarzania danych osobowych w zbiorze osoba administrująca zbiorem informuje ABI. Wprowadzenie zmian wpływających na poziom ochrony danych jest dopuszczalne wyłącznie po wydaniu zgody przez ABI.

Dyrektor na wniosek ABI aktualizuje dokumentację przetwarzania danych. W razie potrzeby należy dokonać aktualizacji wniosku rejestracyjnego zbioru.

### **6.4.3 Wycofywanie z eksploatacji zbioru danych osobowych**

O planowanym zakończeniu przetwarzania danych w zbiorze osoba administrująca zbiorem informuje ABI. Osoba administrująca zbiorem i ABI uzgadniają procedury wycofania zbioru z eksploatacji, zasady przechowywania lub zniszczenia danych ze zbioru. ABI nadzoruje wykonanie uzgodnionych czynności.

Osoba administrująca zbiorem nadzoruje odebranie upoważnień oraz uprawnień związanych z przetwarzaniem danych w wycofywanym z eksploatacji zbiorze.

ABI aktualizuje dokumentację. W razie potrzeby dokonuje wyrejestrowania zbioru.

## **6.5 Obsługa incydentów**

Pracownicy mają obowiązek niezwłocznego zgłaszania incydentów do ABI, a pod jego nieobecność do Dyrektora, lub Kierownika ds. merytorycznych, oraz Specjalisty ds. organizacyjno-administracyjnych<sup>2</sup>, jeśli nastąpiło naruszenie ochrony fizyczno-technicznej obiektu. Zgłoszenia mogą być nadsyłane telefonicznie lub za pośrednictwem poczty elektronicznej.

ABI jest odpowiedzialny za wyjaśnianie skutków i przyczyn zaistniałego incydentu. Z dokonanych ustaleń sporządza notatkę służbową. W przypadku wykrycia naruszenia przepisów o ochronie danych osobowych, w tym naruszenia bezpieczeństwa danych osobowych przedstawia sprawę Dyrektorowi Biblioteki. Dyrektor może podjąć decyzję o ukaraniu pracowników winnych naruszeń lub o skierowaniu zawiadomienia o popełnieniu przestępstwa do organów ścigania.

ABI ewidencjonuje zaistniałe incydenty.

ABI jest odpowiedzialny za zaplanowanie, wdrożenie i nadzorowanie działań naprawczych, korygujących i ew. zapobiegawczych eliminujących skutki i przyczyny zaistniałego incydentu, jeżeli takich działań wymagać będzie bezpieczeństwo danych osobowych. Na podstawie analizy przyczyn incydentów może wnioskować do osób administrujących zbiorami danych lub Dyrektora Biblioteki o wdrożenie dodatkowych zabezpieczeń.

## **6.6 Szkolenia pracowników**

Pracownicy przyjmowani do pracy, upoważnieni do przetwarzania danych osobowych lub do przebywania w pomieszczeniach, w których są przetwarzane dane osobowe są szkoleni przez ABI z zasad ochrony danych

---

<sup>1</sup> tj. zgłoszeniu zbioru do rejestracji, w przypadku, gdy zbiór nie zawiera danych wrażliwych albo w przeciwnym razie zarejestrowaniu zbioru przez GIODO.

<sup>2</sup> Powiadomieni mają obowiązek poinformować ABI o wystąpieniu incydentu tak szybko jak to możliwe.

osobowych oraz przez osoby przyuczające ich na stanowisko pracy z zasad przetwarzania danych osobowych na tym stanowisku. Odbycie szkolenia jest dokumentowane w teczkach osobowych pracowników.

Pracownicy przetwarzający dane osobowe są szkoleni przez ABI z zasad ochrony danych osobowych nie rzadziej niż raz na 2 lata.

ABI ma obowiązek uczestniczyć w szkoleniach i seminariach z zakresu bezpieczeństwa informacji lub ochrony danych osobowych oraz z zakresu bezpieczeństwa systemów informatycznych.

## **6.7 Kontrole przetwarzania danych osobowych**

ABI przeprowadza kontrolę dokumentacji związanej z przetwarzaniem danych osobowych oraz sposób realizacji przyjętych zasad przez pracowników nie rzadziej niż 1 raz w roku. Kontrola obejmuje co najmniej:

- wizje lokalne w placówkach i oddziałach (np. sprawdzenie, czy hasła nie są przechowywane w widocznych miejscach, czy hasła są odpowiednio zmieniane),
- wrywkową znajomość procedur postępowania przez pracowników Biblioteki związanych z ochroną danych osobowych,
- zabezpieczenie systemów informatycznych przetwarzających dane osobowe (w tym aktualność uprawnień do systemów informatycznych, skuteczność tworzenia kopii zapasowych),
- stan zabezpieczeń fizycznych,
- prowadzenie zapisów dotyczących przetwarzania i ochrony danych osobowych.

Z przeprowadzonych działań kontrolnych sporządzany jest protokół, który jest przedstawiany Dyrektorowi Biblioteki. W przypadku wykrycia nieprawidłowości, poza podjęciem działań naprawczych w celu wyeliminowania skutków nieprawidłowości, ABI przeprowadza analizę przyczyn wykrytej nieprawidłowości i rozważa potrzebę przeprowadzenia działań korygujących lub zapobiegawczych, mających 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, ABI we współpracy z osobami administrującymi zbiorami, których te niezgodności lub działania dotyczą, uzgadnia 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.

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

---

## **Załącznik 1. Wzór informacji dla osób, od których pozyskiwane są dane osobowe**

### **Z1. Informacje dla pracowników oraz kandydatów do pracy (przekazywane podczas zbierania danych)**

Administratorem danych jest Biblioteka Publiczna Gminy Kozienice, 26-900 Kozienice, ul. J. Kochanowskiego 22.

Dane wykorzystane będą do realizacji obowiązków pracodawcy wynikających z umowy o pracę lub innej umowy cywilnoprawnej. Przewidywane jest udostępnianie danych Urzędowi Skarbowym, w celu rozliczenia podatku dochodowego od osób fizycznych, Zakładowi Ubezpieczeń Społecznych, w celu przesłania deklaracji ZUS, bankowi w celu realizacji przelewów wynagrodzeń, firmie ubezpieczeniowej w celu ubezpieczenia pracowników.

Obowiązek podania danych wynika z:

- ustawy z dnia 26 czerwca 1974 roku - Kodeks Pracy (Dz.U. 1998 Nr 21 póź. 94 ze zm.),
  - ustawy z dnia 26 lipca 1991 roku o podatku dochodowym od osób fizycznych (Dz.U. 1991 Nr 80 póź. 350 ze zm.),
  - ustawy z dnia 13 października 1998 roku o systemie ubezpieczeń społecznych (Dz.U. 1998 Nr 137 póź. 887 ze zm.).
- Podanie informacji o numerze rachunku bankowego w celu realizacji przelewów o raz deklaracja ubezpieczenia są dobrowolne.

Osobie, której dotyczą dane, przysługuje prawo dostępu do treści tych danych i ich poprawienia.

Potwierdzam zapoznanie się z powyższymi informacjami .....  
(data, czytelny podpis)

(Potwierdzenie nie jest wymagane, jeżeli fakt poinformowania pracownika jest oczywisty - np. gdy klauzula informacyjna znajduje się na wypełnianym przez pracownika formularzu).

### **Z1.2 Informacje dla czytelników (przekazywane podczas zbierania danych)**

Administratorem danych jest Biblioteka Publiczna Gminy Kozienice, 26-900 Kozienice, ul. J. Kochanowskiego 22.

Dane wykorzystane będą do celu zapewnienia ochrony udostępnianych i wypożyczanych zbiorów, dochodzenia ew. roszczeń prawnych, prowadzenia statystyk dot. korzystania z biblioteki. Podanie danych jest dobrowolne ale niezbędne do zarejestrowania i obsługi czytelnika. Udostępnianie danych nie jest przewidywane.

Osobie, której dotyczą dane, przysługuje prawo dostępu do treści tych danych i ich poprawienia.

Potwierdzam zapoznanie się z powyższymi informacjami.....  
(data, czytelny podpis)

(Potwierdzenie nie jest wymagane, jeżeli fakt poinformowania czytelnika jest oczywisty - np. gdy klauzula informacyjna znajduje się na wypełnianym przez pracownika formularzu).

### **Z1.3 Informacje dla czytelników, gdy dane zbierane są od osoby trzeciej (przekazywane podczas zbierania danych)**

Administratorem danych jest Biblioteka Publiczna Gminy Kozienice, 26-900 Kozienice, ul. J. Kochanowskiego 22.

Dane wykorzystane będą do celu zapewnienia ochrony udostępnianych i wypożyczanych zbiorów, dochodzenia ew. roszczeń prawnych, prowadzenia statystyk dot. korzystania z biblioteki. Udostępnianie danych nie jest przewidywane. Dane zostały pozyskane od.....  
Osobie, której dotyczą dane, przysługuje prawo dostępu do treści tych danych i ich poprawienia oraz prawo do wniesienia sprzeciwu wobec przekazywania danych innemu administratorowi danych.

Potwierdzam zapoznanie się z powyższymi informacjami .....  
(data, czytelny podpis)

(Potwierdzenie nie jest wymagane, jeżeli fakt poinformowania czytelnika jest oczywisty - np. gdy klauzula informacyjna znajduje się na wypełnianym przez pracownika formularzu).

### **Z1.4 Informacje dla czytelników (przekazywane w celu wypełnia obowiązku informacyjnego z art. 33 uodo)**

Dane przetwarzane są w Zbiorze Czytelników. Administratorem danych jest Biblioteka Publiczna Gminy Kozienice, 26-900 Kozienice, ul. J. Kochanowskiego 22.

Cel przetwarzania to zapewnienie ochrony udostępnianych i wypożyczanych zbiorów, dochodzenie ew. roszczeń prawnych, prowadzenie statystyk dot. korzystania z biblioteki.

Zakres przetwarzanych danych: imię, nazwisko, nr czytelnika, data urodzenia, zawód, adres zamieszkania, adres zameldowania, nr telefonu, email, dane o rodzicach w przypadku nieletnich, dane osoby upoważnionej do korzystania z konta czytelnika: imię, nazwisko

Dane przetwarzane są w sposób papierowy i w systemie informatycznym.

Data wprowadzenia danych; .....

Treść danych; .....

Źródło danych: osoba, której dane dotyczą

Dane nie zostały /zostały udostępnione; data, zakres, odbiorca .....