Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Stowarzyszeniu Bibliotekarzy Polskich

przyjęta Uchwałą nr 5/2018 Zarządu Głównego Stowarzyszenia Bibliotekarzy Polskich z dnia 21 czerwca 2018 r. (z późniejszymi zmianami)

I. Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

1. „**Polityce bezpieczeństwa**", „**dokumencie**" – należy przez to rozumieć „Politykę bezpieczeństwa w zakresie ochrony danych osobowych w Stowarzyszeniu Bibliotekarzy Polskich";
2. „**Administrator"** oznacza Stowarzyszenie Bibliotekarzy Polskich, który ustala cele i sposoby przetwarzania danych osobowych w SBP;
3. „**SBP"** – oznacza Stowarzyszenie Bibliotekarzy Polskich;
4. „**Dane osobowe"** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą");
5. „**Osoba fizyczna możliwa do zidentyfikowania"** 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;
6. „**Zbiór danych**" oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
7. „**Przetwarzanie"** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich 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;
8. „**Zgoda"** osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
9. „**Naruszenie ochrony danych osobowych"** oznacza 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;
10. „**Osoba upoważniona"** – należy przez to rozumieć: członka SBP, pracownika, współpracownika, wolontariusza, praktykanta SBP posiadającego pisemne upoważnienie do przetwarzania danych osobowych nadane w imieniu Administratora przez przewodniczącego SBP lub upoważnionych przez niego osób;
11. „**System informatyczny"** oznacza zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

12. „**Zabezpieczenie danych w systemie informatycznym”** – należy przez to rozumieć wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
13. „**Usuwaniu danych”** – należy przez to rozumieć zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
14. „**Odbiorcy danych”** – należy przez to rozumieć każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    a) osoby, której dane dotyczą
    b) osoby upoważnionej do przetwarzania danych
    c) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
15. **„Polityce bezpieczeństwa dla bazy członków Stowarzyszenia Bibliotekarzy Polskich”** - należy przez to rozumieć odrębny dokument określający politykę bezpieczeństwa danych osobowych w bazie członków SBP.

II. Wprowadzenie

1. Niniejszy dokument opisuje reguły dotyczące procedur zapewnienia bezpieczeństwa danych osobowych zawartych w systemach informatycznych i zbiorach danych w postaci papierowej w Stowarzyszeniu Bibliotekarzy Polskich.

2. Dokument wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych i jest w szczególności przeznaczony dla osób pracujących przy przetwarzaniu danych osobowych.

3. Dokument określa konsekwencje naruszania zasad ochrony danych osobowych oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

4. Zasady dotyczące przetwarzania danych osobowych w SBP są zgodne z art. 5 RODO (Dz. Urz. UE L 119 z 04.05.2016 r.) . Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);

b) 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;

c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);

d) prawidłowe i w razie potrzeby uaktualniane; Administrator jest zobowiązany podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);

e) 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 w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);

f) 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”).

5. Administrator jest odpowiedzialny za ochronę danych osobowych i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).

III. Ogólne zasady polityki bezpieczeństwa danych osobowych w SBP

1. „Polityka bezpieczeństwa” określa tryb postępowania zapewniający ochronę danych osobowych oraz procedury w przypadku, gdy:

a) stan urządzenia, zawartość rejestru danego zbioru danych osobowych, ujawnione metody pracy mogą wskazywać na naruszenie zabezpieczeń tych danych;

b) stwierdzono naruszenie bezpieczeństwa przetwarzanych danych w rejestrze danego zbioru danych.

2. „Polityka bezpieczeństwa” obowiązuje wszystkie osoby pracujące przy przetwarzaniu danych osobowych w SBP.

3. Zarząd Główny SBP, na mocy Uchwały, wyznacza spośród swoich członków osobę nadzorującą bezpieczeństwo danych osobowych w SBP.

4. W imieniu Administratora za bezpieczeństwo danych osobowych w SBP, zgodnie z niniejszą Polityką Bezpieczeństwa i obowiązującymi przepisami w zakresie ochrony danych osobowych, odpowiada przewodniczący SBP, który upoważnia osoby odpowiedzialne za przetwarzanie określonych zbiorów danych osobowych.

4. 1. Osobami uprawnionymi do otrzymania upoważnienia do przetwarzania danych osobowych są:

a) osoby wchodzące w skład organów statutowych organizacji;

b) pracownicy Biura ZG SBP;

c) członkowie SBP;

d) inne osoby działające na rzecz Stowarzyszenia.

4.2. Przewodniczący SBP udziela w formie pisemnej upoważnienia:

a) administratorom bazy członków SBP;

b) dyrektorowi, głównemu księgowemu i pracownikom Biura ZG SBP;

c) przewodniczącym okręgów do nadawania upoważnień w zakresie ochrony danych osobowych członkom zarządów koła, oddziału i okręgu do przetwarzania odpowiednio danych osobowych zbieranych w strukturach SBP.

4.3. Upoważnienie udzielane jest na czas wykonywania przez osobę upoważnioną czynności na powierzonym stanowisku.

4.4. Wzory upoważnień stanowią odpowiednio załączniki nr 2,3,4,5.

4.5. Administrator może w każdym czasie odwołać w formie pisemnej upoważnienie do przetwarzania danych osobowych.

5. Za ochronę danych osobowych przetwarzanych w Biurze Zarządu Głównego SBP odpowiada Dyrektor Biura.

6. Za politykę bezpieczeństwa bazy członków SBP odpowiada redaktor portalu www.sbp.pl.

7. Za ochronę danych osobowych w kołach, oddziałach i okręgach odpowiada Przewodniczący Zarządu Okręgu i upoważnione przez niego osoby.

8. Upoważnienia osób przetwarzających dane osobowe w Biurze ZG SBP przechowuje osoba upoważniona przez Dyrektora Biura ZG SBP. Ta sama osoba odpowiada za prowadzenie i aktualizację w formie elektronicznej i papierowej ewidencji upoważnień.

9. Ewidencję osób upoważnionych do przetwarzania danych w bazie członków SBP wraz z dokumentacją prowadzi w formie elektronicznej i papierowej redaktor portalu www.sbp.pl.

10. Ewidencję osób wraz z dokumentacją uprawnionych do przetwarzania danych w kołach, oddziałach i okręgach SBP prowadzi osoba upoważniona przez przewodniczącego Zarządu Okręgu.

IV. Zbiory danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

a) wykaz zbiorów danych w Zarządzie Głównym SBP:

1. Baza członków SBP (baza na portalu sbp.pl)

2. Baza użytkowników portalu sbp.pl

3. Dane kadrowe-płacowe pracowników Biura ZG SBP (są rejestrowane w zintegrowanym systemie do zarządzania firmą Raks SQL; system Płatnik służy do przekazywania zbiorczych raportów rozliczeniowych i deklaracji zgłoszeniowych do ZUS)

4. Dane kadrowe-płacowe autorów i współpracowników – umowy cywilno-prawne (są rejestrowane w zintegrowanym systemie do zarządzania firmą Raks SQL; system Płatnik służy do przekazywania zbiorczych raportów rozliczeniowych i deklaracji zgłoszeniowych do ZUS)

5. Dane osobowe niezbędne do prowadzenia działalności szkoleniowej, promocyjnej, organizowanych konkursów

6. Dane osobowe związane z przygotowaniem wniosków o odznaczenia i nagrody (zbiór papierowy; dane przechowywane w programie Word)

7. Dane osobowe osób składających zamówienia w sklepie sbp.pl (forma elektroniczna na portalu sbp.pl)

b) Zakres danych osobowych przetwarzanych w ramach każdego ze zbiorów danych osobowych wymienionych w pkt a)

Ad. 1

Dane osobowe członków SBP, przetwarzane są w formie papierowej oraz elektronicznej i obejmują:

- imiona i nazwiska
- pełny adres domowy lub oznaczenie samej tylko miejscowości
- numer telefonu stacjonarnego i/lub komórkowego i/lub adres poczty elektronicznej
- rok urodzenia
- wykształcenie
- miejsce pracy
- odznaczenia

Ad. 2

Dane użytkowników portalu sbp.pl przetwarzane są w formie elektronicznej na portalu sbp.pl i obejmują:

- imiona i nazwiska
- adres poczty elektronicznej
- nick

Ad.3

Dane osobowe pracowników przetwarzane są w formie elektronicznej w zintegrowanym systemie do zarządzania firmą Raks SQL; do systemu Płatnik są przekazywane raporty zbiorcze dokumentów rozliczeniowych i deklaracji zgłoszeniowych poprzez eksport danych w pliku kedu z systemu Raks SQL.

Dane rejestrowane w systemie Raks SQL obejmują:

- imiona i nazwiska
- pełny adres zameldowania, zamieszkania i do korespondencji
- numer telefonu stacjonarnego i komórkowego oraz adres poczty elektronicznej
- datę urodzenia
- numer ewidencyjny PESEL
- zwolnienia lekarskie
- wysokość wynagrodzenia
- posiadane dzieci

Dane przekazywane do systemu Płatnik obejmują:

- imiona i nazwiska,
- numer ewidencyjny PESEL

- kod ubezpieczenia pracownika.

Ad.4

Dane osobowe autorów i współpracowników przetwarzane są w formie elektronicznej w zintegrowanym systemie do zarządzania firmą Raks SQL; do systemu Płatnik są przekazywane raporty zbiorcze dokumentów rozliczeniowych i deklaracji zgłoszeniowych poprzez eksport danych w pliku kedu z systemu Raks SQL.

Dane rejestrowane w systemie Raks SQL obejmują:

- imiona i nazwiska
- pełny adres zameldowania, zamieszkania i do korespondencji
- numer telefonu stacjonarnego i komórkowego oraz adres poczty elektronicznej
- datę urodzenia
- numer ewidencyjny NIP
- numer ewidencyjny PESEL
- wysokość wynagrodzenia

Dane przekazywane do systemu Płatnik obejmują:

- imiona i nazwiska
- numer ewidencyjny PESEL
- kod ubezpieczenia współpracownika

Ad.5

Dane osobowe niezbędne do prowadzenia działalności szkoleniowej, promocyjnej, organizowanych konkursów (zbiór papierowy i elektroniczny; dane przechowywane w programie Word i Excel) obejmują:

- imiona i nazwiska
- nazwa firmy
- adres firmy
- numer telefonu stacjonarnego i komórkowego oraz adres poczty elektronicznej
- numer ewidencyjny NIP
- wysokość opłaty
- ewentualnie inne dane niezbędne do przeprowadzenia konkursu SBP

Ad.6

Dane osobowe związane z przygotowaniem wniosków o odznaczenia i nagrody (zbiór papierowy; dane przechowywane w programie Word) obejmują:

- imiona i nazwiska
- imiona rodziców
- data i miejsce urodzenia
- miejsce zamieszkania
- wykształcenie
- tytuł naukowy
- miejsce pracy

- zajmowane stanowisko
- staż pracy (ogólnie), w tym staż pracy w bibliotekarstwie
- staż członkowski w SBP
- funkcje pełnione w SBP
- posiadane ordery, odznaczenia
- inne dane wymagane przez instytucje nadające odznaczenia i nagrody

Ad.7

Dane osobowe osób składających zamówienia w sklepie sbp.pl przetwarzane są w formie papierowej i elektronicznej, i obejmują:

- imiona i nazwiska
- pełny adres korespondencyjny
- adres poczty elektronicznej
- numer telefonu

c) wykaz zbiorów danych w przetwarzanych w strukturach terenowych SBP:

1. Baza członków SBP (dostęp do bazy na portalu sbp.pl)

2. Kartoteki z danymi członków SBP (deklaracje wstąpienia do SBP, zbiory papierowe)

3. Dane osobowe niezbędne do prowadzenia działalności szkoleniowej, promocyjnej , organizowanych konkursów, inne (zbiór papierowy; dane przechowywane w programie Word)

4. Dane osobowe związane z przygotowaniem wniosków o odznaczenia i nagrody (zbiór papierowy; dane przechowywane w programie Word).

d) Zakres danych osobowych przetwarzanych w ramach każdego ze zbiorów wymienionych w pkt c) określony jest odpowiednio w pkt b) Ad 1, Ad 5, Ad 6.

V. Pomieszczenia SBP

1. Siedziba Stowarzyszenia Bibliotekarzy Polskich - Zarząd Główny, wpisana do KRS znajduje się w Warszawie, ul. Konopczyńskiego 5/7, mieści się tam Wydawnictwo Naukowe i Edukacyjne SBP. Lokal jest monitorowany, w oknach są kraty. Biuro Zarządu Głównego SBP ma siedzibę w Warszawie, al. Niepodległości 213 (w siedzibie Biblioteki Narodowej). Lokal jest monitorowany i zabezpieczony zgodnie z zasadami obowiązującymi w Bibliotece Narodowej. Drzwi są zabezpieczone zamkami, klucze oddawane są do portierni BN.

SBP zajmuje pokoje o numerach:

338,339 – Dział Sprzedaży i Promocji

337 – Kadry, Dział Finansowy (gromadzą i przetwarzają dane osobowe)

336 – Portal SBP (prowadzi bazę członków SBP)

336 – Sekretariat (gromadzi wybrane dane osobowe dot. członków SBP oraz dane osobowe związane z przygotowywaniem wniosków o odznaczenia państwowe, resortowe, stowarzyszeniowe)

335 - Dyrekcja

2. Pomieszczenia, gdzie przechowywane są dane osobowe wyposażone są w szafy drewniane zamykane na zamek. Dodatkowo w pokoju 337 znajduje się metalowy sejf z zamkiem szyfrowym. Dostęp do poszczególnych pomieszczeń mają pracownicy Biura Zarządu Głównego SBP zajmujący dane pomieszczenie, a także osoby z zewnątrz (sprzątające pomieszczenia, obsługa techniczna). Lista osób uprawnionych do odbioru kluczy z portierni Biblioteki Narodowej znajduje się w biurze ochrony Biblioteki Narodowej.

3. Struktury terenowe SBP (koła, oddziały i okręgi) nie posiadają własnych pomieszczeń. Swoje siedziby mają w bibliotekach, które im użyczają szafy do przechowywania dokumentacji.

VI. Środki organizacyjne i techniczne ochrony danych osobowych

1. Administrator jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych i na nośnikach tradycyjnych, a w szczególności do:

a) zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym;

b) zapobiegania kradzieży danych;

c) zapobiegania przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

2. Do zastosowanych przez Administratora i osoby przez niego upoważnione w Stowarzyszeniu Bibliotekarzy Polskich środków organizacyjnych służących zapewnieniu poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych należy:

a) opracowanie i wdrożenie „Polityki bezpieczeństwa w zakresie ochrony danych osobowych w Stowarzyszeniu Bibliotekarzy Polskich”;

b) nadanie członkom organów SBP, pracownikom, współpracownikom, wolontariuszom, praktykantom i stażystom SBP upoważnień do przetwarzania danych osobowych;

c) nadawanie pracownikom i współpracownikom organizacji upoważnień do przetwarzania danych osobowych w związku z realizacją projektów/zadań, w których organizacja będzie partnerem (niezależnie od tego, czy lider projektu/zadania [realizator] udzieli takiego upoważnienia, czy też nie);

d) nadawanie pracownikom i współpracownikom organizacji upoważnień do przetwarzania danych osobowych w pozostałych przypadkach przetwarzania danych osobowych występujących w organizacji;

e) sprawowanie przez osoby wyznaczone przez Administratora kontroli i nadzoru nad procesem przetwarzania danych osobowych oraz ich udostępniania.

3. Do zastosowanych środków organizacyjnych należą następujące zasady:

a) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed jej przystąpieniem do pracy przy przetwarzaniu danych osobowych;

b) przeszkolenie osób upoważnionych w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych;

c) kontrolowanie otwierania i zamykania pomieszczeń wymienionych w pkt V, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę i niepozostawianiu pomieszczenia w czasie pracy bez nadzoru.

4. Do zastosowanych środków technicznych należy:

a) przetwarzanie danych osobowych w wydzielonych, odpowiednio zabezpieczonych i przystosowanych do tego pomieszczeniach;

b) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt 1;

c) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji i nośników danych.

5. Dla potrzeb ochrony danych osobowych przetwarzanych w SBP w formie papierowej stosuje się zabezpieczenia polegające na przechowywaniu:

- dokumentacji bieżącej – np. w szafach zamykanych na zamki w obszarach przetwarzania danych osobowych
- dokumentacji archiwalnej i dokumentacji pracowniczej – np. w specjalnie do tego celu przeznaczonym pomieszczeniu (najczęściej archiwum Biblioteki, w której jednostka główna lub terenowa ma siedzibę).

6. W przypadku zewnętrznych (obcych) systemów informatycznych dla potrzeb bieżącego użytkowania i przesyłania danych stosowane są zabezpieczenia podmiotów, którym przekazywane są dane:

- „Płatnik” (program ZUS) – organizacja posiada certyfikowany publiczny klucz dostępu do tego programu wydany na czas określony, ponadto co 30 dni zmieniane jest hasło dostępu do programu (program przypomina o upływie terminu ważności hasła), gwarancję zachowania poufności danych stanowi także ograniczony krąg osób upoważnionych do jego obsługi: główna księgowa i samodzielny księgowy. Hasła i loginy są przechowywane w sejfie.
- Zintegrowany system do zarządzania firmą Raks SQL posiada licencję na oprogramowanie i jest zabezpieczony hasłem użytkownika, dostęp do systemu za pomocą odrębnych haseł posiadają: specjalista ds. sprzedaży, samodzielny księgowy i główna księgowa. Hasła i loginy są przechowywane w sejfie.
- Przelewy bankowe i międzybankowe – strona internetowa banku, w którym organizacja posiada rachunki wymaga podania loginu i hasła (kod zmieniający się co minutę z wykorzystaniem urządzenia o nazwie Token), osoby upoważnione do dokonywania przelewów: główna księgowy i samodzielny księgowy. Hasła i loginy są przechowywane w sejfie.

7. Komputery firmowe są zabezpieczone licencjonowanymi programami antywirusowymi: Kaspersky i ESET NOD32.

8. Niezależnie od niniejszych zasad, w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych

oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie, przy czym dokumenty te nie mogą być sprzeczne z przepisami prawa oraz z regulacjami określonymi w „Polityce bezpieczeństwa".

9. Administrator za pośrednictwem osoby wymienionej w punkcie III.4 sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

10. Raz w roku osoba sprawującą nadzór nad przestrzeganiem ochrony danych osobowych wymieniona w pkt III.4 sporządza raport o stanie ochrony danych osobowych w SBP i przedstawia Zarządowi Głównem SBP .

VII. Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Za rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji uważa się niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych itp.

2. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako naruszenie obowiązków pracowniczych, w szczególności przez osobę, która po stwierdzeniu naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym fakcie Administratora.

4. W przypadku stwierdzenia :

a) naruszenia zabezpieczeń systemu informatycznego
b) naruszenia technicznego stanu urządzeń
c) naruszenia zawartości zbioru danych osobowych
d) ujawnienia metody pracy lub sposobu działania programu
e) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych
f) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

<u>każda osoba zatrudniona przy przetwarzaniu danych osobowych jest zobowiązana niezwłocznie powiadomić o tym fakcie odpowiednio Dyrektora Biura ZG SBP, a w przypadku naruszeń poza Biurem ZG SBP, odpowiednio przewodniczącego Zarządu Okręgu/Oddziału.</u>

5. W razie niemożliwości zawiadomienia Dyrektora Biura ZG SBP lub osób upoważnionych w okręgach/oddziałach, należy powiadomić bezpośredniego przełożonego.

6. Do czasu przybycia na miejsce naruszenia danych osobowych upoważnionej osoby, należy:

a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia – o ile istnieje taka możliwość – a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców naruszenia danych osobowych
b) udokumentować wstępnie zaistniałe naruszenie
c) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia osoby przez upoważnionej.

7. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, osoba upoważniona:

a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy organizacji
b) może żądać dokładnej relacji z zaistniałego naruszenia lub ujawnienia ochrony danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem
c) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu lub ujawnieniu ochrony danych osobowych
d) nawiązuje bezpośredni kontakt – jeżeli zachodzi taka potrzeba – ze specjalistami spoza organizacji.

8. Po wyczerpaniu niezbędnych środków doraźnych związanych z zaistniałym naruszeniem/ujawnieniem ochrony danych osobowych, Dyrektor Biura lub odpowiednio osoba upoważniona zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

9. Dyrektor Biura lub osoba upoważniona dokumentuje zaistniały przypadek naruszenia lub ujawnienia ochrony danych osobowych oraz sporządza raport, który powinien zawierać w szczególności:

a) wskazanie osoby powiadamiającej oraz innych osób zaangażowanych lub odpytywanych w związku z naruszeniem lub ujawnieniem ochrony danych osobowych

b) określenie czasu i miejsca: naruszenia/ujawnienia i powiadomienia o tym fakcie

c) określenie okoliczności towarzyszących i rodzaju naruszenia/ujawnienia

d) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania

e) wstępną ocenę przyczyn wystąpienia naruszenia/ujawnienia

f) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

10. Raport, o którym mowa w pkt. 9, Dyrektor Biura lub osoba upoważniona niezwłocznie przekazuje przewodniczącemu SBP oraz członkowi Zarządu Głównego SBP sprawującemu nadzór nad przetwarzaniem danych osobowych w SBP (pkt III.4).

11. Zaistniałe naruszenie/ujawnienie ochrony danych osobowych może stać się przedmiotem szczegółowej analizy prowadzonej przez Administratora.

12. Analiza, o której mowa w pkt. 11, powinna zawierać:

a) wszechstronną ocenę zaistniałego naruszenia/ujawnienia ochrony danych osobowych;

b) wskazanie odpowiedzialnych;

c) wnioski co do ewentualnych przedsięwzięć: proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom/ujawnieniom w przyszłości.

VIII. Postanowienia końcowe

1. Wdrożenie „Polityki bezpieczeństwa" odbywa się poprzez:

a) zapoznanie osób wchodzących w skład organów organizacji, pracowników, współpracowników, wolontariuszy, praktykantów i stażystów organizacji z treścią „Polityki bezpieczeństwa";

b) w szczególnych przypadkach, szkolenia z zakresu ochrony danych osobowych.

2. Osoby upoważnione do przetwarzania danych SBP, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych, potwierdzają ten fakt poprzez podpisanie Oświadczenia (załącznik nr 1 do „Polityki bezpieczeństwa").

3. „Polityka bezpieczeństwa" wchodzi w życie z dniem podjęcia Uchwały Zarządu Głównego SBP lub w terminie określonym w treści tej Uchwały.

4. Zmiany w „Polityce bezpieczeństwa" będą będą podejmowane w Uchwałach Zarządu Głównego SBP.

4.1. Zmiany wynikające ze zmiany przepisów lub innych okoliczności (np. zmiana siedziby, oprogramowania, itp.) są podejmowane w Uchwałach Prezydium ZG SBP.

4.2. Zmiany są dokumentowane w Arkuszu Zmian Polityki Bezpieczeństwa w zakresie ochrony danych osobowych w Stowarzyszeniu Bibliotekarzy Polskich.

Załącznik nr 1: Oświadczenie osoby upoważnionej o zapoznaniu się z „Polityką bezpieczeństwa w zakresie ochrony danych osobowych w Stowarzyszeniu Bibliotekarzy Polskich"
Załącznik nr 2: Upoważnienie dla administratorów bazy członków SBP
Załącznik nr 3: Upoważnienie dla Przewodniczącego Zarządu Okręgu do udzielania upoważnień przetwarzania danych osobowych członkom zarządów kół/oddziałów/okręgu.
Załącznik nr 4: Upoważnienie do przetwarzania danych osobowych w kołach/oddziałach/okręgach
Załącznik nr 5: Upoważnienie do przetwarzania danych osobowych pracowników Biura ZG SBP
Załącznik nr 6: Zgoda na przetwarzanie danych osobowych
Załącznik nr 7: Karta informacyjna SBP, zgodnie z art. 13 RODO (Dz. Urz. UE L 119 z 04.05.2016 r.)